

ELSA MicroLink™ Cable

Manual

© 1999 ELSA AG, Aachen (Germany)

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. ELSA shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from ELSA. We reserve the right to make any alterations that arise as the result of technical development.

ELSA is DIN EN ISO 9001 certified. The accredited TÜV CERT certification authority has confirmed ELSA conformity to the worldwide ISO 9001 standard in certificate number 09 100 5069, issued on June 15, 1998.

Trademarks

Windows®, Windows NT® and Microsoft® are registered trademarks of Microsoft, Corp.

All other names mentioned may be trademarks or registered trademarks of their respective owners. The ELSA logo is a registered trademark of ELSA AG.

Subject to change without notice. No liability for technical errors or omissions.

ELSA AG
Sonnenweg 11
52070 Aachen
Germany

ELSA, Inc.
2231 Calle De Luna
Santa Clara, CA 95054
USA

www.elsa.com

Aachen, October 1999

Preface

Thank you for placing your trust in this ELSA product.

With the *ELSA MicroLink Cable*, you have chosen a modem that will open the door to the Internet for you with unparalleled speeds and remain online permanently.

The highest quality standards in manufacturing and stringent quality control are the basis for high product standards and consistent product quality.

This documentation contains the following chapters:

- Introducing the *ELSA MicroLink Cable*
- Installation and configuration
- Configuration modes
- Operating modes and functions
- Technical basics
- Technical reference
- Appendix



Our online services (Internet server www.elsa.com) are available to you around the clock should you have any queries regarding the topics discussed in this manual or require any further support. In the Support file section under 'Know-How', you can find answers to frequently asked questions (FAQs). The KnowledgeBase also contains a large pool of information. Current drivers, firmware, tools and manuals can be downloaded at any time.

The KnowledgeBase can also be found on the CD. Just open the file `\\Misc\\Support\\MISC\\ELSASIDE\\index.htm`.

Content

Introducing the <i>ELSA MicroLink Cable</i>	1
The <i>ELSA MicroLink Cable</i> takes the stage.....	1
What does the unit look like?	1
Node or hub?	3
The highlights of the <i>ELSA MicroLink Cable</i>	4
Fast Internet	4
Internet at all times—always online	5
More than just Internet.....	5
CE conformity and FCC radiation standard	7
Installation and Configuration	9
First Steps	10
Quick Start: Quick configurations	11
Preparations	11
Configuration as a bridge	11
Configuration as a router	13
Set up the workstation computers (Windows 95 or 98).....	15
Configuration modes	17
The user-friendly method: inband.....	17
Requirements for inband configuration	17
Alternatively: addresses can be managed by the DHCP server	17
Starting inband configuration using <i>ELSA LANconfig</i>	18
Start up inband configuration using telnet.....	18
Configuration commands	19
What's happening on the line?.....	21
Trace Outputs.....	21
New firmware with FirmSafe	22
This is how FirmSafe works.....	22
How to load new software	23
Configuration using SNMP	24
General.....	24
Accessing tables and parameters using SNMP	25
The Management Information Base (MIB)	27
Operating modes and functions	29
Security for your configuration	29
Password protection	29
Login barring	29
Access control via TCP/IP	30

Security for your LAN.....	30
Encryption	31
TCP/IP packet filters	31
The hiding place—IP masquerading (NAT, PAT)	31
IP routing	32
The IP routing table.....	32
Dynamic routing with IP RIP	34
Local routing	35
IP masquerading (NAT, PAT).....	36
DNS forwarding	38
Bridging.....	39
Automatic address administration with DHCP.....	40
The DHCP client	41
The DHCP server	41
DHCP – 'on', 'off' or 'auto'?	42
How are the addresses assigned?	42
Technical basics	47
Cable modem technology	47
Standards	47
Access.....	47
Registration in the cable network	48
Network technology.....	50
The network and its components	50
Connection modes	50
Kinds of networks	52
IP addressing.....	52
IP routing and hierarchical IP addressing	55
Expansion through local networks.....	57
Appendix	63
Technical data	63
Warranty conditions	65
Declaration of conformity	67
Description of the menu options	73
Status.....	75
Status/Operating-time	76
Status/Current-time	76
Status/cable-statistics.....	76
Status/LAN-statistics	77
Status/bridge statistics	78
Status/TCP-IP-statistics	79

Status/IP-router-statistics	83
Status/config statistics.....	85
Status/Queue-statistics	85
Status/MCNS-statistics.....	87
Status/Init-status	87
Status/DHCP-client-statistics	88
Setup	88
Setup/cable-module	89
Setup/LAN-module	89
Setup/bridge-module	90
Setup/TCP-IP-module	91
Setup/IP-router-module	94
Setup/SNMP-module	101
Setup/DHCP-server-module	101
Setup/Config-module	103
Firmware	104
Other	106

Introducing the *ELSA MicroLink Cable*

Internet access is the main application for the *ELSA MicroLink Cable*. The operator of the cable network to which you have connected your modem may offer additional services or regional information.

This chapter describes the display elements and connections of the modem, accessing the Internet, and the characteristics and techniques that ensure fast, secure data exchange.

The precise use of the *ELSA MicroLink Cable*'s features will be explained in the following sections and with the aid of the examples in the 'Workshop'.



The term 'router', as used in the remainder of the manual, refers to the router functions of our ELSA MicroLink Cable.

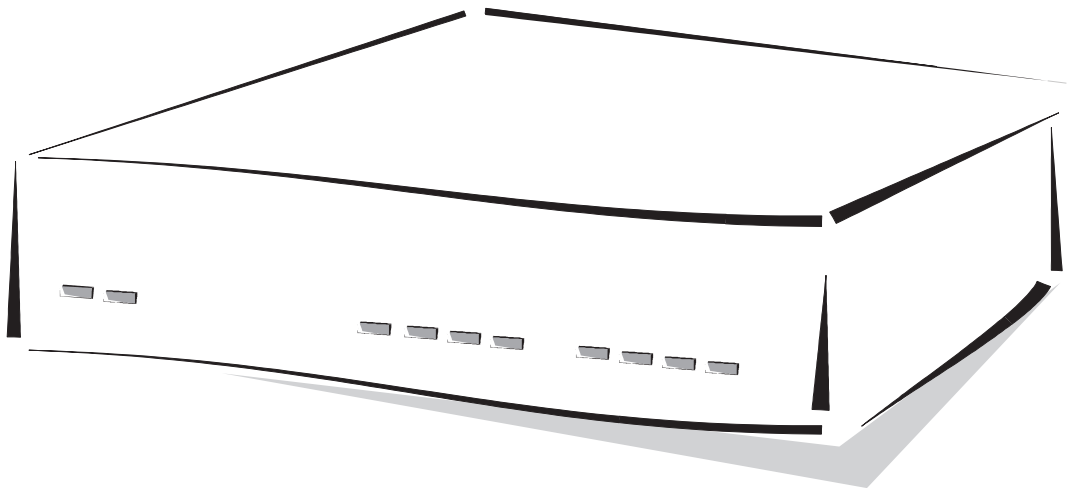
The *ELSA MicroLink Cable* takes the stage

This section introduces the unit's hardware. It covers the unit's display elements and connection options.

What does the unit look like?

We would first like to familiarize you with the device.

You will find a number of LEDs as display elements on the front panel.



ON

This LED flashes once when the power supply is switched on. After the self-test, either an error is output by a flashing light code or the device starts and the LED remains lit.

Off		Unit switched off, power supply plugged in
red	1 x short	Boot procedure (test and load) started
red	flashing	Display of a boot error (flashing light code)
red		Device ready for use

Standby

This LED shows that the unit is in stand-by mode. The *ELSA MicroLink Cable* is registered with the cable network provider in this state, but there is no active connection to the local network. In other words, no data can be exchanged between the Internet and the LAN in this state.

The *ELSA MicroLink Cable* can be switched to this mode by configuring the function of the power switch correspondingly and then actuating this switch on the rear of the unit.

Cable-Tx, -Rx, -Sync, Reg'd

These LEDs display the status of the interface to the cable network:

Cable-Tx	yellow	Data packet sent from the device to the Internet
Cable-Rx	green	Data packet received from the Internet
Cable-Sync	green	The device has found a channel on which it can communicate with the cable network operator's headend.
Cable-Reg'd	green	The registration and all required negotiations between the unit and the headend have been completed and the registration confirmed by the headend. The unit is ready to exchange data with the Internet in this state.

Blink codes

The Sync and Reg'd LEDs can display the various phases of the cable modem registration through combined blink codes, thus offering configuration troubleshooting information. The meanings of the specific blink codes:

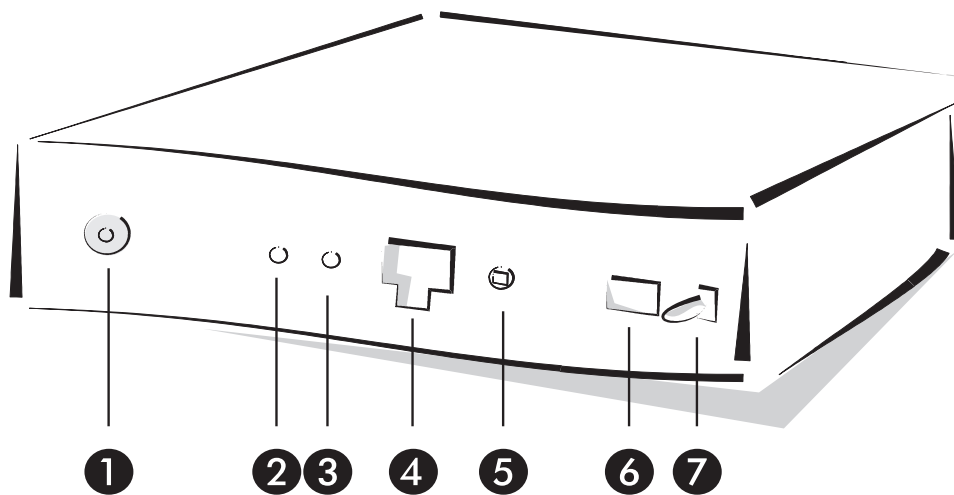
SYNC	REG'd	What has been achieved so far?	What is the modem trying to do?
off	off		channel search with 64/256QAM channel
1 pulse	off	QAM lock	FEC lock
2 pulse	off	FEC lock	TRC lock
on	off	TRC lock	initial ranging
on	1 pulse	initial ranging	DHCP
on	2 pulse	DHCP	ToD
on	3 pulse	ToD	Configuration file
on	4 pulse	Configuration file	Registration
on	on	Registration	

LAN-Tx, -Rx,
LAN-Coll, -Link

These LEDs show the corresponding network controller status:

LAN -tx	yellow	Data packet sent from the device to the LAN
LAN-Rx	green	Data packet received from the LAN
LAN coll	red	Sending collision
LAN-Link	green	Connection to LAN is established and ready

Now turn the whole thing around and take a look at the rear. Beginning again on the left-hand side, you have:



- 1 Connector for the cable TV network (CATV)
- 2 Reset switch—performs a hardware reset
- 3 Factory Default button—the unit's factory defaults are restored after holding this button for approx. 15 seconds
- 4 10Base-T network connection
- 5 Node/hub selector switch
- 6 Connection for power supply unit
- 7 On/standby switch

Node or hub?

Please check the position of the Node/Hub switch when connecting the unit to the LAN:

- As the factory default, the switch is set to 'Node'. In this setting, the device acts as a node on a network. It can, in this case, only be connected to a hub, not directly to the network card of a computer.
- Set the switch to 'Hub' if you do not wish to connect the device to a hub but directly to a workstation. In this setting the lines for sending and receiving the data are crossed.



Look at the link status LED (Link) to check if the node/hub switch is set correctly.

The highlights of the *ELSA MicroLink Cable*

The cable modem is a new Internet-access technology that is now competing with conventional modems, Internet modems and small ISDN routers. To take maximum advantage of your *ELSA MicroLink Cable*, you should know the areas and characteristics in which cable modems have the technological edge.

Fast Internet

Cable modems use a split transfer rate depending on the direction of the signals. Downstream refers to the transfer of data from the network operator to the participant, upstream is the opposite direction. This asymmetrical split is quite acceptable, since users generally receive far more information from the Internet than they send to it.

Cable network

Up to 43 Mbps can be transferred downstream; upstream transfer speeds reach up to 10 Mbps.

Shared media: This colossal performance is shared by up to 2000 users connected to the same cable section, however. This is referred to as the use of a shared media.
Multiple users share a single "cable"

Bandwidth: The data flow in the cable network does not take place at a constantly high volume, but in irregular intervals. Also, it's unlikely that all 2000 participants will be using the network simultaneously, so the available bandwidth is certainly adequate to ensure the fast transfer of data.
Throughput, transfer capacity

The cable network operators have the option of limiting the available bandwidth for individual participants, or offering several channels with 43 Mbps each. Please contact your network operator for further information on transfer rates and pricing models.

Backbone

Backbone:
*direct
connection to
the Internet*

The simple transfer rate between the network operator and participant does not by itself determine the speed at which the Internet can be accessed. The network operator must also forward data destined for the Internet to a backbone. The dimensioning of this connection ultimately determines the speed at which you can surf. The backbone can become a bottleneck if a large number of participants want to access Internet data simultaneously and the network operator does not have an adequately dimensioned connection to the Internet.

Internet at all times—always online

One of the biggest advantages of cable modem technology is the continuous availability of the Internet. While “normal” Internet connections need to be established as required, all cable modem users on a cable section can be permanently registered with the headend. The multiport capabilities of the remote stations ensure that other participants are not blocked due to a lack of connections. The advantages of this permanent Internet connection:

- Immediate availability of all information

Your e-mail comes to you directly—not just when you pick it up. To view a Web page, just open your browser and don't worry about connecting to your provider.

- Your own Internet server

Until now, running your own Internet server generally meant having an extremely expensive leased line to the provider. Now you have one! If you would like to set up your own Web server for your company, you can now do so and have it accessible at all times via the cable modem at no additional cost.

More than just Internet

Together with the appropriate remote stations, cable modems form the connection between network participants (private or business) and the network operator. Very high throughputs—and thus very fast data transfers—can be realized using such a connection. In addition to providing fast Internet access, this creates a number of other interesting options for the evolution of network operators into information service providers.

Regional content

Cable network operators generally have a local or regional orientation due to the structure of the cable network. The headends that have to be additionally integrated into the network with their restriction to around 2000 participants results in further area limitations.

Network operators can take advantage of this structure to provide regional content in addition to the Internet. This can be accomplished by setting up Web servers that do not need to be accessible from the Internet. These can then be used for special information services for network participants, such as the programs of local cinemas, regional news, information for clubs and special-interest groups, and so on—essentially, everything that is of interest to the regional cable network participants, but that might be superfluous on the Web.

Proxy servers

The network operator can also use local servers to speed up access to the Internet. These proxy servers are used for the intermediate storage of information from the Internet.

Proxy: *Stand-in* Every page requested from the Internet by participants in the local cable network section is stored in this proxy server for a specific period of time. As a rule, the storage period on the proxy server is determined by the cable network operator. If another participant requests the same page, the proxy server can serve the page directly without having to find it on the Internet first.

This is generally beneficial, for example by speeding up downloads considerably. However, when calling up information subject to frequent changes such as stock prices, accessing the current Web page is usually a must. In such a case the version of the page stored on the proxy server can already be out of date or incorrect. If this could be relevant to you, please check with your network operators whether they deploy proxy servers. Clicking the **Refresh** button will download the current information directly from the Internet, however.

CE conformity and FCC radiation standard

CE

This equipment has been tested and found to comply with the limits of the European Council Directive on the approximation of the laws of the member states relating to electromagnetic compatibility (89/336/EEC) according to EN 55022 class B and EN55024.

FCC

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the Federal Communications Commission (FCC) Rules. Operation is subject to the following two conditions:

- ❶ This device may not cause harmful interference, and
- ❷ This device must accept any interference received, including interference that may cause undesired operation.

The FCC ID of this device is KJGMLCABLE.

CE and FCC

These limits are designed to provide reasonable protection against radio frequency interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may interfere with radio communications if not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception (this can be determined by turning this equipment off and on), the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between this equipment and the receiver.
- Connect the equipment to an outlet on a circuit other than that to which the receiver is connected.
- Consult your dealer or an experienced radio/TV technician.
- Caution: To comply with the limits for an FCC Class B computing device, always use a shielded signal cable.



The Federal Communications Commission warns the user that changes or modifications to the unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Installation and configuration

The aim of this chapter is to get you online as quickly as possible. First please check that the contents of the package are complete:

- *ELSA MicroLink Cable*
- Power supply
- Twisted-pair LAN connector cable
- WAN connector cable (coaxial) or corresponding adapter
- Documentation
- CD containing *ELSA LANconfig* and electronic documentation

Computers to be connected to the Internet using this device must fulfill the following requirements:

- Any operating system that supports the TCP/IP network protocol, such as Windows 95, Windows 98, Windows NT 4.0, OS/2, Linux, BeOS
- Windows 95, Windows 98 or Windows NT 4.0 and a CD-ROM drive on the computer on which you would like to install the *ELSA LANconfig* configuration software.
- Ethernet network adapter
- TCP/IP network protocol installed and bound to the network adapter

First, we will show you how to connect your new *ELSA MicroLink Cable*, how to install the *ELSA LANconfig* configuration software and perform the initial configuration. The unit will then be ready to connect your computer or network to the Internet.

If this is all going too fast for you or you're not familiar with the technical terms, you can also find further information in this documentation, such as detailed descriptions of the unit and its functions, sample configurations, descriptions of the software, glossaries, etc.



This unit is designed to be connected to the broadband cable TV network. The connection is made using the supplied coaxial cable or the appropriate adapter.

First Steps

1 Give it some power

First, give your device the power it needs through the power supply unit!

2 Onto the net

Connect the unit to your local network using the twisted pair cable. Please check the position of the node/hub switch: 'Node' is the correct position when connecting the unit to a network. Switch to 'Hub' when connecting the unit directly to a workstation.

3 The wire to the world

Connect the *ELSA MicroLink Cable* to the TV cable network using the coaxial cable or the adapter and a normal antenna cable. Data is transmitted through the cable TV network in accordance with the MCNS (**M**ultimedia **C**able **N**etwork **S**ystem)/DOCSIS standard.



The connection to the cable TV network must provide a certain signal level. This value will be checked by your cable network operator and adjusted as required.

4 And we're off

Switch the device on at the back. The 'Power' LED on the front panel lights up after a short self-test. The 'LAN Link' LED indicates that the unit is correctly connected to the LAN and that the Node/Hub switch is correctly set.



If this LED is not lit, change the position of the Node/Hub switch. If the LED still does not light up, there may be a problem with the network adapter or the cabling.

5 Software installation

The *ELSA LANconfig* configuration software for Windows 95, Windows 98 or Windows NT 4.0 may be used to configure the unit as required or to set it up for other applications. Alternatively, you can perform the configuration via telnet from any other TCP/IP capable computer (e.g. Linux, Solaris). Install the TCP/IP network protocol, followed by the *ELSA LANconfig* on the computer that will be used to set up the device. If the setup program does not start up automatically after insertion of the CD, start Windows Explorer, click on 'autorun.exe' on the *ELSA MicroLink Cable* and follow the instructions in the install program.

6 Configuring the *ELSA MicroLink Cable*

The first time *ELSA LANconfig* is run, the new modem is automatically detected on the TCP/IP network and can immediately be configured.

When configuring the router with *ELSA LANconfig*, you can use the setup wizards to quickly and conveniently guide you through the required settings.

Quick Start: Quick configurations

We're sure that after you've installed the hardware and software, you'll want to get going quickly without bothering with technical details. In the following sections, we'll show you how to set up your *ELSA MicroLink Cable* quickly for the most common applications—without bothering with the whys and wherefores.

After the preparations that you should check in any case, we will introduce the configuration of the unit as a bridge and IP router. Further information on the bridge and router functions can be found in the 'Operating Modes' chapter.

Preparations

The Internet is based on the TCP/IP network protocol. The individual devices in the Internet (workstations, servers, routers, etc.) are identified using unique IP addresses. All computers exchanging data on the Internet therefore must have the TCP/IP network protocol installed and must be assigned a valid IP address.

IP addresses can either be manually entered, permanently for each computer, or assigned automatically by a different computer, a so-called DHCP server. Your cable network operator has such a DHCP server, and one is also contained in the *ELSA MicroLink Cable* itself. For this quick-start, we prefer using the automatic assignment of an IP address by a DHCP server. The cable network operator's DHCP server will be used when configuring the unit as a bridge; in router mode the integrated DHCP server of the *ELSA MicroLink Cable* will be used.

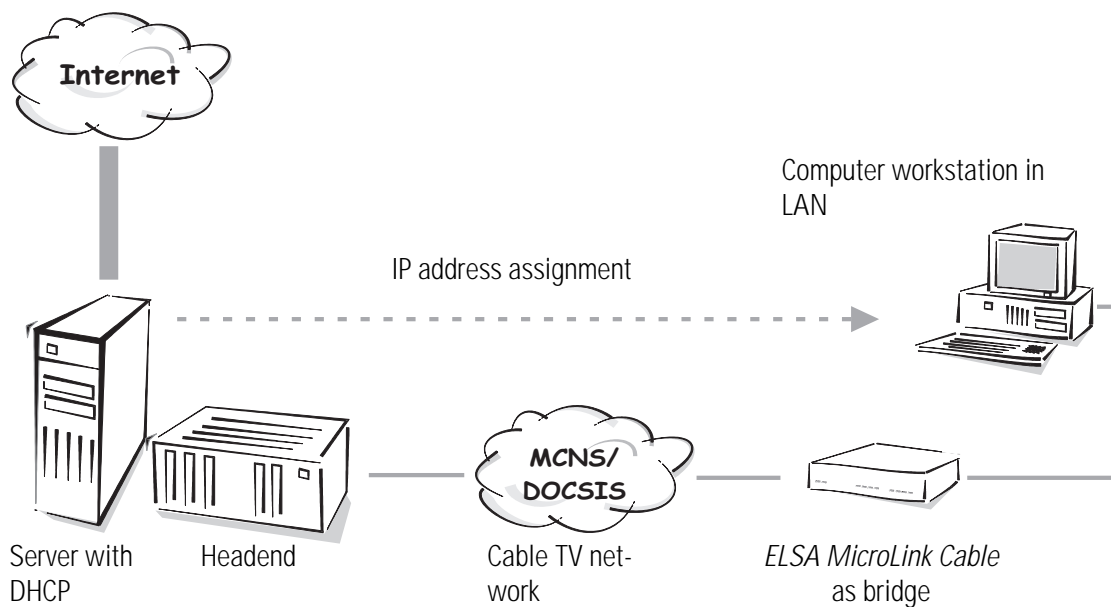
The following settings are required regardless of the operating mode you intend to use with your *ELSA MicroLink Cable*:

- Install the TCP/IP network protocol on all computers on the network.
- Activate the automatic assignment of IP addresses via DHCP for the workstations (generally the default setting).

Just how you do that will be explained in section 'How to set up the workstation computers' towards the back of this chapter.

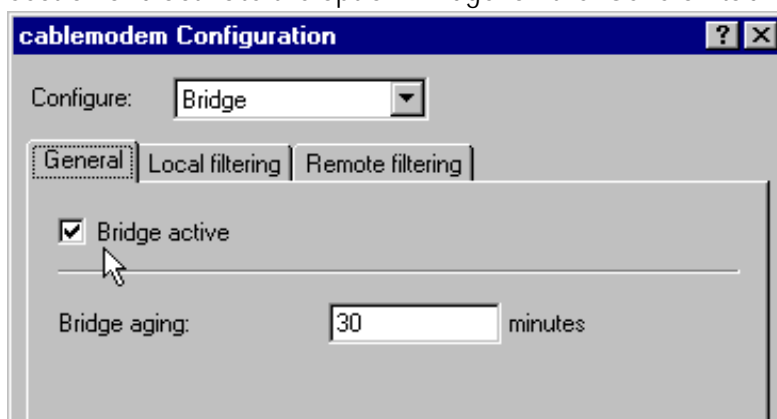
Configuration as a bridge

Bridge mode is the simplest configuration for the *ELSA MicroLink Cable*. In this mode, the unit does not take IP addresses into consideration and transfers all data that is not destined for workstations in the local network directly to the Internet. In the opposite direction, all data coming from the Internet for a specific computer in the local network is transferred (insofar as that computer has already sent data to the Internet). It's thus not necessary to worry about the assignment of IP addresses. The computers in your local network receive their IP addresses directly from the DHCP server of the cable network operator.



In this example, only one computer is connected to the Internet via the ELSA MicroLink Cable. In principle however, several computers can be connected to the ELSA MicroLink Cable, using a hub for example, if the network operator permits.

- ① Start up *ELSA LANconfig* by clicking **Start** ► **Programs** ► **ELSAlan** ► **ELSA LANconfig**.
- ② Click the entry for the *ELSA MicroLink Cable* in the device list to open the configuration dialog. If an entry doesn't exist yet, create a new one using **Device** ► **New**. For the IP address, enter '10.0.0.254' or 'x.x.x.254', in which 'x.x.x' stands for the addresses previously in use in your network, if applicable. Go to the 'Bridge' section and activate the option 'Bridge' on the 'General' tab.



- ③ Go to the 'TCP/IP' configuration section and on the 'Router' tab, disable the 'IP Router' option. Also deactivate the DHCP server of your *ELSA MicroLink Cable* on the 'DHCP Server' tab, as well as the 'IP Masquerading' function on the 'Masquerading' tab.
- ④ Save the configuration with **OK**.

The *ELSA MicroLink Cable* is now ready for use in bridge mode. Open your Web browser, and off you go into the Web with a whole new sensation of speed...

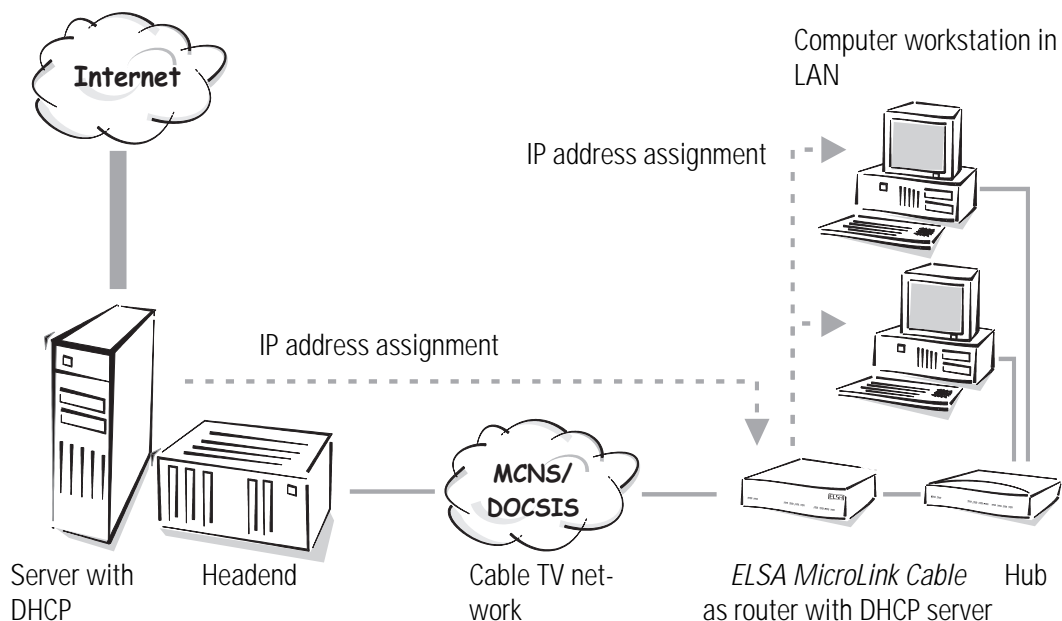


If you can only access the Internet with a single computer while using this configuration, your cable network operator may have placed a limit on the maximum number of connected computers. Either ask your network operator to increase the number, or configure your ELSA MicroLink Cable as a router (with DHCP server and IP masquerading).

If necessary, filters can be defined to restrict the exchange of data packets between the local network and the Internet.

Configuration as a router

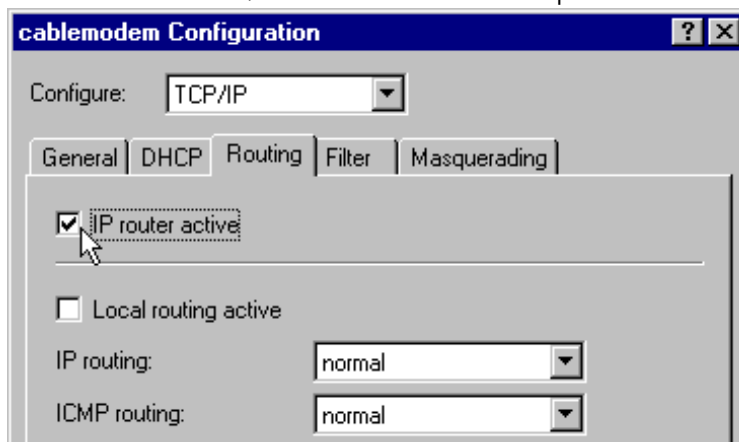
In addition to bridge mode, the *ELSA MicroLink Cable* can also serve as an IP router. In this mode, the *ELSA MicroLink Cable* pays careful attention to the IP addresses of the computers exchanging data with the Internet. The exchange of data with the Internet can thus be set up with much greater precision in this mode. The DHCP server and IP masquerading functions will assist you with the administration of IP addresses in the LAN.



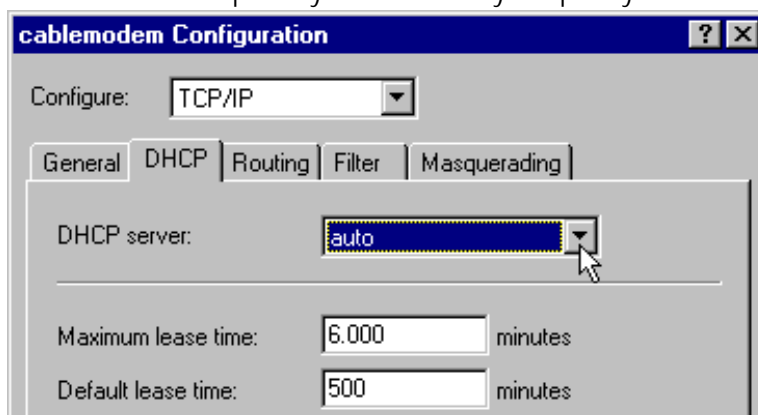
In this example, several computers are connected to the ELSA MicroLink Cable, and thus to the Internet, using a hub. In principle however, a single computer can also be connected directly to the ELSA MicroLink Cable.

- ① Start up *ELSA LANconfig* by clicking **Start ► Programs ► ELSAan ► ELSA LANconfig**.

- ② In order for a device to be able to assign addresses to other devices on a TCP/IP network, it first needs an IP address valid in the LAN itself (LAN-IP address). Click the entry in the device list to open the configuration dialog. If an entry doesn't exist yet, create a new one using **Device ► New**. For the IP address, enter '10.0.0.254' or 'x.x.x.254', in which 'x.x.x' stands for the addresses previously in use in your network, if applicable. Switch to the 'TCP/IP' configuration section and on the 'General' tab, enter the LAN IP address and the associated netmask.
 - If you have not used any IP addresses on your network so far, you can assign any address you like from the address space reserved for private use, e.g. '10.0.0.1' with the subnet mask '255.255.255.0'. You are thereby also defining the address space that the DHCP server will use for the other devices on the network.
 - If you have already configured IP addresses on the computers on the LAN, allocate a free address to the device from the address space you used previously.
- ③ On the 'Router' tab, enable the 'IP Router' option.



- ④ On the 'Masquerading' tab, enable the 'IP Masquerading' function. This will conceal the IP addresses in use in your local network from the Internet. This protects your network from intruders and avoids conflicts with other networks that may be using the same addresses internally (also see IP addressing and IP masquerading).
- ⑤ Go to the 'DHCP' tab and set the DHCP server to Auto mode. This lets the unit handle the local IP address administration by itself. The *ELSA MicroLink Cable* determines the valid address pool by itself unless you specify otherwise.



- ⑥ Go then to the 'Bridge' section and deactivate the option 'Bridge' on the 'General' tab.
- ⑦ Save the configuration with **OK**.

The *ELSA MicroLink Cable* is now ready for use in router mode. Open your Web browser, and off you go into the Web with a whole new sensation of speed...

If necessary, filters can be defined to restrict the exchange of data packets between the local network and the Internet. This lets you define restrictions on the workstations that can access the Internet, or on specific pages of the Internet that cannot be viewed.



Set up the workstation computers (Windows 95 or 98)

We will now briefly show you how the workstation computers must be set up (e.g. under Windows 95 and Windows 98) to ensure problem-free communication between the computers on the TCP/IP network and the router, if this has not already been done.

■ TCP/IP installation

Install TCP/IP by clicking **Start ► Settings ► Control Panel ► Network ► Add ► Protocol**. Select 'Microsoft' under Manufacturers and 'TCP/IP' under Network Protocols.

■ Obtain IP addresses automatically (use DHCP)

Here's how to set individual workstations to automatically obtain an IP address: **Start ► Settings ► Control Panel ► Network ► TCP/IP ► Properties ► IP Address ► Obtain an IP address automatically**. Delete any existing entries for DNS servers and gateways on the 'Gateway' and 'DNS Configuration' tabs and disable the 'DNS' option. When rebooting, the workstation will look for a DHCP server in the network and will allow the server to assign it an IP address and a netmask.

■ Configuring fixed IP addresses (not using DHCP)

If you do not wish to use a DHCP server on your network you should configure fixed IP addresses on your workstation computers: **Start ► Settings ► Control Panel ► Network ► TCP/IP ► Properties ► IP Address ► Specify an IP address**.

Allocate unique IP addresses, e.g. from a reserved address space. The workstations can be assigned the addresses '10.1.1.2' to '10.1.1.253', for example, the *ELSA MicroLink Cable* the address '10.1.1.1', all with the netmask '255.255.255.0'. Ensure that the address intended for the *ELSA MicroLink Cable*, i.e. '10.1.1.1', is available by opening a DOS box and entering the command `ping 10.1.1.1`. If you do not receive a reply to this request the address is probably still unused.



Assign fixed IP addresses in router mode with activated IP masquerading only. Otherwise, address conflicts with other users in your cable network may result when using router mode without IP masquerading, or bridge mode.

- Specifying the gateway and the DNS server (not necessary if using DHCP)

Enter the LAN IP address of the *ELSA MicroLink Cable* in your own local network as the gateway and domain name server (DNS server) in the individual workstations:

Start ► Settings ► Control Panel ► Network ► TCP/IP ► Properties ► Gateway and DNS Configuration. You must also specify a host name for the DNS configuration. Use the name of the PC for reasons of consistency, which, for example, could be the same as the user name.

- Checking the IP configuration

Check the current IP configuration of the computer under Windows 95 or Windows 98 by selecting **Start ► Run ► winipcfg**. Among other information, you can see the IP address assigned to the computer by the DHCP server and the addresses conveyed for the DNS server and gateway.

IP Configuration

Host Information

Host Name: ST171

DNS Servers:

Node Type: Hybrid

NetBIOS Scope Id:

IP Routing Enabled: ☐ WINS Proxy Enabled: ☐

NetBIOS Resolution Uses DNS: ☐

Ethernet Adapter Information

Ethernet Adapter: ELNK3 Ethernet Adapter

Adapter Address: 00-20-AF-BE-99-A3

IP Address: 193.103.233.171

Subnet Mask: 255.255.255.0

Default Gateway:

DHCP Server:

Primary WINS Server:

Secondary WINS Server:

Lease Obtained:

Lease Expires:

OK Release Renew Release All Renew All

Configuration modes

ELSA cable modems are always delivered with up-to-date software in which a number of the settings have already been prepared for you.

It will nevertheless be necessary for you to add some information and configure them to your specific needs. These settings are made as part of the configuration process.

This section will show you the programs and routes you can use to access the device and set it up.

And, if the team at ELSA has produced firmware with new features, we will show you how to load the new software.

The user-friendly method: inband

Using inband configuration allows any computer on the cable network or LAN to access the router. However, this is only possible if the router permits it, as access from the WAN or LAN can be restricted or completely blocked by the IP access list. Inband configuration requires the use of either telnet (supplied with most operating systems) or the *ELSA LANconfig* configuration program for Windows. *ELSA LANconfig* is supplied with your device. You can always obtain up-to-date releases from our online media.

Requirements for inband configuration

TCP/IP or TFTP are used to make configurations using telnet or *ELSA LANconfig*. The TCP/IP protocol must therefore be installed on the computer being used and your cable modem must be given an IP address which you will then use when addressing it.

A device that has not been configured yet will respond to the IP address XXX.XXX.XXX.254, in which the Xs are placeholders for the network address in your LAN. If the computers on your network have addresses such as 192.110.130.1, then you will be able to address the router using 192.110.130.254.



If a computer with the address XXX.XXX.XXX.254 is already active on your network, shut down the computer with this IP address before continuing. Give the device a new LAN IP address as soon as you have established a connection to it, using ELSA LANconfig or telnet.

Alternatively: addresses can be managed by the DHCP server

If it is not absolutely essential that you configure the correct IP addresses manually, the DHCP server can perform this task for you automatically. When using the DHCP server you can have the IP addresses for all computers on the network assigned automatically (see also chapter 'Automatic Address Administration with DHCP').

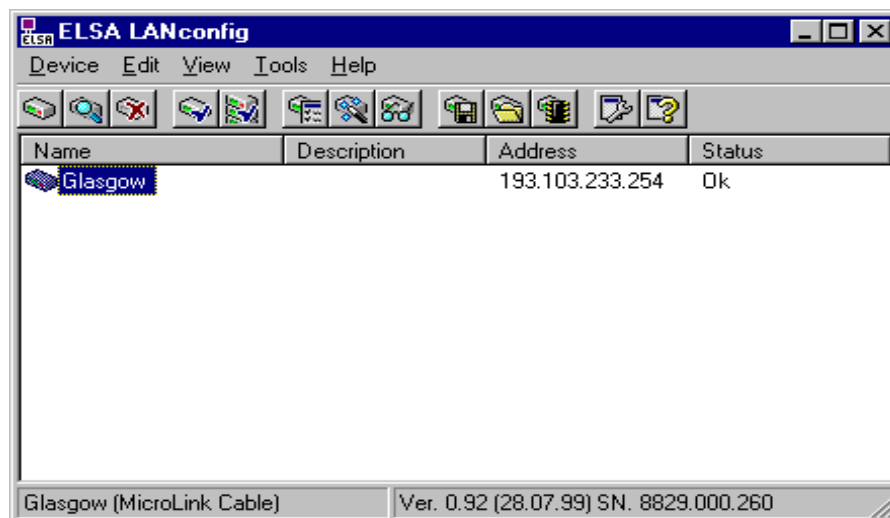
Starting inband configuration using *ELSA LANconfig*

After the installation (double-click on 'autorun.exe') is complete, call up the *ELSA LANconfig* configuration tool, for example by clicking on **Start ► Programs ► ELSAlan ► ELSA LANconfig** in the Windows task bar. *ELSA LANconfig* searches the local area network for *ELSA MicroLink Cable* devices.



Just click on the **Find** button or call up the command with **Device ► Find** to initiate a search for a new device manually. *ELSA LANconfig* will then prompt you for a location to search. You will only need to specify the local area network if using the inband solution, and then you're off.

Once *ELSA LANconfig* has finished its search, it displays a list of all the devices it has found, together with their names and a description if available, the IP address and its status.



Double-clicking the entry for the highlighted device and then clicking the **Configure** button or the **Edit ► Edit Configuration File** option reads the device's current settings and displays the general device information.

The remainder of the program's operation is essentially self-explanatory or covered in the online help. You can click on the question mark top right in any window or right-click on an unclear term at any time to call up context-sensitive help.

Start up inband configuration using telnet

Start inband configuration using telnet with the command from a DOS box:

```
telnet 10.1.80.125
```

Telnet will then establish a connection with the device using the IP address.


After the entry of the password (if you specified one to protect the settings) all commands from the 'Configuration Commands' section are available.

Configuration commands

Enter commands and path specifications using the normal DOS or UNIX conventions if you are using telnet or a terminal program to configure the device.

Enter a forward slash or backslash to separate the path specifications. You do not need to write out commands and table entries in full; an unambiguous abbreviation will do.

The entries for the categories MENU, VALUE, TABLE, TABINFO, ACTION and INFO will be displayed while configurations are made and may be modified. You can use the following commands to do this:

This command means this for instance:
? or help	Calls up help text	-
dir, list, ll, ls <MENU>, <VALUE> or <TABLE>	Displays the contents of MENU, VALUE or TABLE	dir/status/wan-statistics displays the current WAN statistics
cd <MENU> or <TABLE>	Switches to the MENU or TABLE specified	cd setup/tcp-ip-module (or cd se/tc for short) switches to the TCP/IP module
set <VALUE>	This resets the VALUE.	set IP-address 192.110.120.140 sets a new IP address
	Insert a space between all entries in table rows. An * leaves the entry unchanged.	set /setup/name AACHEN assigns the name 'AACHEN' to the device.
set <VALUE> ?	Shows you which values can be specified here	
del <VALUE>	Deletes a table row.	del /se/wan/nam/AACHEN Deletes the entry for the remote station AACHEN.
do <ACTION> (parameters)	Executes the ACTION according to any parameters specified,	do /firmware/firmware-upload starts the upload of new firmware.
passwd	Allows a new password to be specified. The old password, if there is one, must be entered first. The new password must then be entered twice and confirmed each time with  .	
repeat <sec> <ACTION>	Repeats the ACTION at an interval of the number of seconds specified. Any key can be used to terminate the repetition.	repeat 3 dir/status/wan-statistics displays the current WAN statistics every 3 seconds
time	Sets the system time and date.	time 24.12.1998 18:00:00
language <language>	Sets the language for the current configuration session.	Languages currently supported: English (language english) German (language deutsch)
exit, quit, x	Configuration is terminated.	

Text entries with spaces are only accepted if they are placed in quotation marks, e.g.
`set /se/snmp/admin "The Administrator".`

Text entries (individual and table values) can be deleted as follows:

```
set /se/snmp/admin " "
```

What's happening on the line?

Trace Outputs

Trace outputs may be used to monitor the internal processes in the cable modem during or after configuration.



The trace outputs are slightly delayed behind the actual event, but are always in the correct sequence. This will not usually hamper interpretation of the displays but should be taken into consideration if making precise analyses.

How to start a trace

The command to call up a trace follows this syntax:

```
trace [code] [parameters]
```

The trace command, the code, the parameters and the combination commands are all separated from each other by spaces. And what is lurking behind the code and parameters?

This code in combination with the trace causes the following:
?	Displays a help text
+	Switches on a trace output
-	Switches off a trace output
#	Switches between different trace outputs (toggle)
no code	Displays the current status of the trace

This parameter brings up the following display for the trace:
Status	Status messages for the connection
Error	Error messages for the connection
IP router	IP routing
IP-RIP	IP Routing Information Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
Masquerade	Processes in the masquerading module
DHCP	Dynamic Host Configuration Protocol

This combination command	... brings up the following display for the trace:
All	All trace outputs
Display	Status and error outputs

This combination command	... brings up the following display for the trace:
TCP-IP	IP-Rt., IP-RIP, ICMP and ARP outputs
Time	Displays the system time in front of the actual trace output
Source	Includes a display of the protocol that has initiated the output in front of the trace.

Any appended parameters are processed from left to right. This means that it is possible to call a parameter and then restrict it.

Examples

This code in combination with the trace causes the following:
trace	Displays all protocols that can generate outputs during the configuration, and the status of each output (ON or OFF)
trace + all	Switches on all trace outputs
trace + all - icmp	Switches on all trace outputs with the exception of the ICMP protocol
trace - time	Switches off the system time output before the actual trace output.



You will find notes on the interpretation of trace outputs in the reference section of this guide.

New firmware with FirmSafe

The software for the devices of ELSA is constantly being updated. We have fitted the units with a flash ROM which makes child's play of updating the operating software so that you can enjoy the benefits of new features and functions. No need to change the EPROM, no need to open up the case: simply load the new release and you're away.

This is how FirmSafe works

FirmSafe makes the installation of the new software safe: The current firmware is not simply overwritten but saved additionally in the device as a second firmware.

Only one of the firmware versions stored in the device can be active at any one time. When new firmware is loaded the inactive firmware is overwritten. You can decide which firmware version you want to activate after the upload:

- 'Immediate': The first option is to load the new firmware and activate it immediately. The following situations can result:
 - The new firmware is successfully loaded and then operates as desired. Everything is then in order.

- The device no longer responds after loading the new firmware. If an error occurs during the upload, the router automatically reactivates the previous firmware version and reboots the device.
- 'Login': To avoid problems with faulty uploads there is the second option with which the firmware is uploaded and also immediately booted.
 - The difference to the first option is that the router then waits five minutes for a successful login to the device via outband or inband (via telnet). Only if this login attempt is successful does the new firmware remain active permanently.
 - If the device no longer responds and it is therefore impossible to log in, the router automatically loads the previous firmware version and reboots the device with it.
- 'Manual': With the third option you can define a time period during which you want to test the new firmware yourself. The router will start with the new firmware and wait for the preset period until the loaded firmware is manually activated and therefore becomes permanently effective.

How to load new software

There are various ways of carrying out a firmware upload (which is the term given to the installation of software), all of which produce the same result:

- Configurations tool *ELSA LANconfig* (recommended)
- Terminal programs
- TFTP



All settings will remain unchanged by a firmware upload. All the same you should save the configuration first for safety's sake (with **Edit ► Save Configuration to File** if using *ELSA LANconfig*, for example).

If the newly installed release contains parameters which are not present in the device's current firmware, the router will add the missing values using the default settings.

ELSA LANconfig



When using the *ELSA LANconfig* configuration tool, highlight the desired device in the selection list and click on **Edit ► Firmware Management ► Upload New Firmware**, or click directly on the **Firmware Upload** button. Then select the directory in which the new version is located and mark the corresponding file.

ELSA LANconfig then tells you the version number and the date of the firmware in the description and offers to upload the file. The firmware you already have installed will be replaced by the selected release by clicking **Open**.

You also have to decide whether the firmware should be permanently activated immediately after loading or set a testing period during which you will activate the firmware yourself. To activate the firmware during the set test period, click on **Edit ► Firmware Management ► Upload New Firmware**.

TFTP

With TFTP you can use the **writelflash** command to install new firmware. To send a new firmware version which, for example, is in the 'LC_1000U.130' file, to a router with the IP address 194.162.200.17, you would enter the following command under Windows NT for example:

```
tftp -i 194.162.200.17 put lc_1000u.130 writelflash
```



*This command sends the corresponding file to the router using the **writelflash** parameter. Binary file transfer must be set for TFTP. However, many systems have the ASCII format preset. This example for Windows NT shows you how to achieve this by using the '-i' parameter.*

The device is booted up following a successful firmware upload and this activates the new firmware switch directly. If an error occurs during the upload (write error in the flash ROM, TFTP transmission error or similar) the device also boots and FirmSafe activates the previous firmware. The configuration remains in operation.

It will only be possible to configure the device locally, i.e. via the outband interface, if it is switched off during TFTP upload. The device will expect a firmware upload via the serial port when it is switched back on.



You should therefore be sure to carry out a firmware upload only when you have a secure (stable) connection.

With TFTP, other configuration commands can also be executed. The syntax is best demonstrated with the following examples:

- `tftp 10.0.0.1 get readconfig file1` : Reads the configuration from the device with the address 10.0.0.1 and saves it as file1 in the current directory
- `tftp 10.0.0.1 put file1 writeconfig` : Writes the configuration from file1 to the device with the address 10.0.0.1
- `tftp 10.0.0.1 get dir/status/verb file2` : Saves the current connection information in file2

Configuration using SNMP

General

The Simple Network Management Protocol (SNMP V.1 as specified in RFC 1157) allows monitoring and configuration of the devices on a network from a single central instance. This instance is commonly termed the "Manager" while the devices become "Agents". The structure permitted for SNMP information exchange is relatively simple. A manager can access all SNMP-capable devices and services (agents) on the network. The access rights are controlled via "Communities".

SNMP V.1 has only a very limited set of commands at its disposal, as the table below shows:

Command	Target/Source	Function
GetRequest	Manager – Agent	retrieves information from the agent
GetNextRequest	Manager – Agent	retrieves the information contained in the following MIB from the agent
SetRequest	Manager – Agent	modifies a setting in the agent
GetResponse	Agent – Manager	returns the queried value to the manager
Trap	Agent – Manager	reports on an error or special status

These commands can be used for central monitoring and configuration of SNMP-capable devices on a network. The SNMP capabilities of the agents are specified in so-called MIBs = Management Information Bases.

The firmware of ELSA routers includes an implementation for an SNMP V.1 agent (in accordance with RFC 1157). A part of MIB-2 and a private MIB, included in the product as a separate file, are supported. This MIB must be loaded and translated by an SNMP manager (HP OpenView, for example) to allow you to manage a device completely using SNMP. All menus and parameters of the remote configuration will then be available to you on a single branch of the SNMP management tree:

Accessing tables and parameters using SNMP

Any of the tables and parameters can be read and modified as necessary via the SNMP interface. This also involves specifying in the MIB the variables which should have 'read-only' or 'read-write' status. Commercially available SNMP managers indicate 'read-only' and 'read-write' status using color coding.

Access protection in SNMP V.1

Access to SNMP objects is controlled using so-called communities. A community is basically a password used to govern access to particular classes of information. The router permits read-only access to all parameters and tables through the 'public' community. Bear in mind that this community cannot execute any write accesses.

You must use the device's password if you wish to write data using SNMP. Write access using SNMP will **not** be granted as a matter of principle if the device's password is not entered.

If the trapping mechanism is enabled and a failed access attempt is detected, an 'Authentication Failed' trap is triggered and sent to the manager(s) in the SNMP trap table.

Bear in mind that the access protection given by the community mechanism in the SNMP V.1 is only very limited since the data, the MIB IDs and the communities are not encrypted in the UDP data blocks of requests and responses as they are transmitted.

Deleting rows in tables using SNMP

SNMP itself has no mechanisms intended for deleting. You therefore have to use a trick to delete entries from tables.

If you need to delete a row, you have to change the index entry value, i.e. the value in the first column, to its current value.

- Example: You want to delete the 3rd row from following IP routing table.

IP address	IP-netmask	Router name	Distance
192.168.0.0	255.255.0.0	0.0.0.0	0
172.16.0.0	255.240.0.0	0.0.0.0	0
10.0.0.0	255.0.0.0	ROBERT	0
224.0.0.0	224.0.0.0	0.0.0.0	0

The entry '10.0.0.0' (i.e. the first cell of the third row) is amended in the manager to its current value, i.e. to '10.0.0.0', and the Set command is sent off. The SNMP SetRequest now contains the command to amend the first cell of the third row to '10.0.0.0'. The SNMP software recognizes that this assignment to the index is redundant and interprets it as a delete command.

Appending rows to tables using SNMP

There are two ways of inserting rows in a table:

- Using the set command will result in a new row through setting a new index entry. By using the command in the syntax:
`someTable.1.2.2 = xyz`
 a row with index '2' will be generated in the table 'someTable', with the entry 'xyz' in its second column. The '1' after the table name is constant for this command and stands for 'someEntry' in the SNMP-Syntax.
- When using SNMP managers that do not allow the entry of index values, it is possible to amend any existing index entry to the new index value of the new row. The row which has been used as the source for the amendment will itself remain unchanged.

If we take Castlerock SNMPc as an example, the first possibility can be realized as follows:

- ① Activate the **Display MIB Table** item in the **Manage** menu of Castlerock SNMPc.

- ② Open the corresponding table. If the table is empty, then empty columns will be displayed.
- ③ Click on **Edit**. It is now possible to display the values for every single column in the table.
- ④ Enter the index of the table and the value for the column to be subsequently placed, and click on **Set** at the right-hand side of the latter column.

A new column with the new index and the value for another column should now appear.



*It is also possible to enter values for all columns of the row and simultaneously place all columns, using **Set All**.*

This procedure can also be carried out using **Edit MIB Vars..** in the **Manage** menu. In this case, click through to the table, single-click on the column to be placed, enter the index in the field **Variable Name** after the name of this column and the new value in **Variable Value**. After clicking Set, a new table row should appear.

Error messages via SNMP trap

Error or warning messages can be sent to a manager using the SNMP mechanism. The SNMP agent contained in the router permits traps to be sent to up to 20 SNMP managers. The IP addresses of these managers are configured in the Configuration menu under `/setup/SNMP-module/IP-Trap-Table`. You can enable and disable the transmission of trap messages using the `/setup/SNMP-module/Send-Traps` switch.

The Management Information Base (MIB)

A textual representation of the configuration structure (the so-called private MIB) must be supplied with the *ELSA MicroLink Cable* so that the SNMP management system can access its configuration. The syntax of this MIB complies with ASN.1 (Abstract Syntax Notation One, ISO 8824). There is usually a so-called MIB compiler included with the SNMP management software. This compiler converts the MIB file into a form that can be used by the manager.

The current ELSA MIB can be found both included with the product on CD and in the ELSA online media.

Operating modes and functions

This section is an introduction to the functions and operating modes of your device. It includes information on the following points:

- Security for your configuration
- Security for your LAN
- IP routing
- Bridging
- DHCP server

Along with the description of the individual points, we will also give you information to support you as you configure your device.

Detailed sample configurations can be found in the Workshop.

Please refer to the electronic documentation for a detailed description of all parameters and menus.

Security for your configuration

A number of important parameters for the exchange of data are established in the configuration of the device. These include the security of your network, monitoring of costs and the authorizations for the individual network users.

Needless to say, the parameters that you have set should not be modified by unauthorized persons. The *ELSA MicroLink Cable* thus offers a variety of options to protect the configuration.

Password protection

The simplest option for the protection of the configuration is the establishment of a password. As long as a password hasn't been set, anyone can change the configuration of the device.

The password input field can be found in the configuration tool *ELSA LANconfig* in the 'Management' configuration section on the 'Security' tab. The password prompt can be activated in a terminal or telnet session in the `/Setup/Config-Module/passw.prompt` menu. In this case, the password itself is set with the command `passwd`.

Login barring

The configuration in the *ELSA MicroLink Cable* is protected against "brute force attacks" by barring logins. A brute-force attack is the attempt of an unauthorized person to crack

a password to gain access to a network, a computer or another device. In order to do so, a computer can, for example, go through all the possible combinations of letter and numbers until the right password is found.

As a measure of protection against such attacks, the maximum allowed number of unsuccessful attempts to Login can be set. If this limit is reached, the access will be barred for a certain length of time.

These parameters apply globally to all configuration options (telnet, TFTP/*ELSA LANconfig* and SNMP). If barring is activated on one port all other ports are automatically barred too.

The following entries are provided in the configuration tool *ELSA LANconfig* for configuring login barring in the 'Management' configuration area on the 'Security' tab or under `/Setup/Config-Module` in the menu:

- 'Lock configuration after' (`Login-errors`)
- 'Lock configuration for' (`Lock-minutes`)

Access control via TCP/IP

Access to the internal functions of the devices through TCP/IP can be restricted using a special filter list. Internal functions in this case means Telnet or TFTP sessions to configure the *ELSA LANconfig*.

This table is empty by default and so access to the router can therefore be obtained by TCP/IP using Telnet or TFTP from computers with any IP address. The filter is activated when the first IP address with its associated network mask is entered and from that point on only those IP addresses contained in this initial entry will be permitted to use the internal functions. The circle of authorized users can be expanded by inputting further entries. The filter entries can describe both individual computers and whole networks.

The access list can be found in the configuration tool *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'General' tab, or in the `/Setup/TCP-IP Module/Access List` menu.

Security for your LAN

You certainly would not like any outsider to access or edit the data on your computers. A *ELSA MicroLink Cable* offers you various ways of restricting access from outside:

- Data encryption
- Data packet filtering
- IP masquerading (also known as NAT or PAT)

Encryption

Since cable modems transfer data via a cable shared by many participants, data should be encrypted to prevent access by the other participants.

All data between the modem of the provider and the modem of the end users is automatically transferred in an encrypted state. This is where the DES encryption (Data Encryption Standard) with a code length of 56 comes in. In addition, the code in use is repeatedly changed during the transfer of data. This guarantees the highest level of protection.

TCP/IP packet filters

You can use your entries in the routing table to determine quite precisely which data should be transferred. Additionally, you can use a special entry in the 'Router-name' field to reject whole groups of IP addresses.

Occasionally, you may wish to restrict a transmission even further. You can do this using a characteristic of TCP/IP, which is to send port numbers for destination and source as well as the source and destination IP addresses with a data packet. The destination port in a data packet stands for the service to be addressed in the TCP/IP network. The destination ports are fixed for the various services on the TCP/IP network. The source ports, on the other hand, may be selected freely within certain ranges.

The IP router can check the source and destination ports of data packets using the TCP or UDP protocols. It can then deduce the purpose of the data from these ports. For example, FTP accesses or Telnet sessions can be identified. The appropriate filter table can be used to determine that certain data is not to be transferred from the LAN to the remote station. Data for particular ports can also be blocked from entering the LAN in the same way.

In addition to the definition of the port range and the associated protocols, the filter table can be used to determine whether the data packet concerned will be accepted or rejected. Both interfaces of the cable modem (for the cable network and for the LAN) can be set separately for incoming and outgoing data transfer.

This filter table can be found in the configuration tool *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Filter' tab, or in the `/Setup/IP router/firewall menu`.

The hiding place—IP masquerading (NAT, PAT)

One of today's most common tasks for a cable modem is connecting the numerous workstation computers in a LAN to the ultimate network, the Internet. Everyone should have the potential to access the WWW from his workstation and be able to fetch bang up-to-date information for his work.

But this provokes objections from the network manager responsible for the security of data on the company's network: Every workstation computer on the WWW? Surely this means that anyone can get in from outside?—Not true!

IP masquerading provides a hiding place for every computer while connected with the Internet. Only the router module of the unit and its IP address are visible on the Internet. The computers in the LAN then use the router as a gateway so that they themselves cannot be detected. To do this, the router separates Internet and intranet, as if by a wall. Therefore, IP masquerading is also called a “firewall function”.

For further information, see the 'IP Routing: IP masquerading' section.

IP routing



This chapter describes the function of the cable modem as an IP router. Whenever the IP router (or simply the router) is mentioned in the next paragraphs, this is a reference to the corresponding operating mode of the cable modem.

An IP router works between networks which use TCP/IP as the network protocol. This only allows data transmissions to destination addresses entered in the routing table. This chapter explains the structure of the IP routing table of an ELSA router, as well as the additional functions available to support IP routing.

The IP routing table

Use the IP routing table to tell the router which remote station (which other router or computer) it should send the data for particular IP addresses or IP address ranges to. This type of entry is also known as a “route” since it is used to describe the path of the data packet. This procedure is also called “static routing” since you make these entries yourself and they remain unchanged until you either change or delete them yourself. Naturally, there is also “dynamic routing” too. The routers use the routes in this way to exchange data between themselves and continually update it automatically. The static routing table can hold up to 64 entries, the dynamic table can hold 128. The IP router looks at both tables when the IP/RIP is activated.

The routing table can be found in the configuration tool *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Router' tab, or in the `/Setup/IP router/IP routing` menu. This, then, is how an IP routing table might look:

IP address	IP netmask	Router	Distance
192.168.0.0	255.255.0.0	0.0.0.0	0
172.16.0.0	255.255.0.0	0.0.0.0	0
10.0.0.0	255.0.0.0	0.0.0.0	0

IP address	IP netmask	Router	Dis- tance
224.0.0.0	224.0.0.0	0.0.0.0	0
255.255.255.255	0.0.0.0	CABLE	1
192.168.130.0	255.255.255.0	192.168.140.123	1

What do the various entries on the list mean?

■ IP addresses and IP network masks

This is the address of the destination network to which data packets may be sent and its associated network mask. The router uses the network mask and the destination IP address of the incoming data packets to check whether the packet belongs to the destination network in question.

The route with the IP address "255.255.255.255" with a network mask of "0.0.0.0" is the default route. Any data packets which cannot be routed by other routing entries are transmitted via this route.

■ Router Name

The router name indicates what should be done with the data packets that correspond to the IP address and the network mask.

Routes with the router name "0.0.0.0" describe Exclusion routes. Data packets for this "zero route" are rejected and are not routed any further. This is how routes which are forbidden on the Internet (private address spaces, e.g. 10.0.0.0), for example, are excluded from transmission.

If a router name consists of an IP address, this means we are dealing with a locally accessible router, responsible for the transmission of the appropriate data packets.

By default, you will find the entry „CABLE“ in the cable modem, as a router name at the default route. All IP data packets transferred via this route are forwarded to the cable interface.

■ Distance

Number of routers between your own and the destination router.

Examples with explanatory notes:

IP address	IP netmask	Router name	Dist.	This is what happens:
192.168.130.0	255.255.255.0	192.168.140.123	0	All data packets with destination IP addresses 192.168.130.x are transmitted to the locally accessible router with the IP address 192.168.140.123.

IP address	IP netmask	Router name	Dist.	This is what happens:
192.168.0.0	255.255.0.0	0.0.0.0	0	Excludes transmission of all data packets to networks using private address spaces.
172.16.0.0	255.255.0.0	0.0.0.0	0	
10.0.0.0	255.0.0.0	0.0.0.0	0	
224.0.0.0	224.0.0.0	0.0.0.0	0	
255.255.255.255	0.0.0.0	CABLE	1	All data packets which cannot be allocated to the entries listed above are transmitted into the cable network.

Dynamic routing with IP/RIP

In addition to the static routing table ELSA routers also have a dynamic routing table containing up to 128 entries. Unlike the static table, you do not fill this out yourself, but leave it to be dealt with by the router itself. It uses the Routing Information Protocol (RIP) for this purpose. This protocol is used by all devices with RIP to exchange information regarding the reachable routes.

What information is propagated by IP/RIP?

A router uses the IP/RIP information to inform the other routers in the network of the routes it finds in its own static table. The following entries are ignored in this process:

- Rejected routes with the '0.0.0.0' router setting.
- Routes referring to on other routers in the local network.

Which information does the router take from received IP/RIP packets?

When the router receives such IP/RIP packets, it incorporates them in its dynamic routing table, which looks something like this:

IP address	IP netmask	Time	Distance	Router
192.168.120.0	255.255.255.0	1	2	192.168.110.1
192.168.130.0	255.255.255.0	5	3	192.168.110.2
192.168.140.0	255.255.255.0	1	5	192.168.110.3

What do the entries mean?

IP addresses and network masks identify the destination network, the distance indicates the number of routers between sender and receiver, the final column indicates the router which announced this route. This leaves the 'Time'. The dynamic table thus shows how old the relevant route is. The value in this column acts as a multiplier for the intervals at which the RIP packets arrive. A '1', therefore, stands for 30 seconds, a '5' for about 2.5 minutes and so on. New information arriving about a route is, of course, designated as directly reachable and is given the time setting '1'. The value in this column is

automatically incremented when the corresponding amount of time has elapsed. The distance is set to '16' after 3.5 minutes (route not reachable) and the route is deleted after 5.5 minutes.

Now if the router receives an IP/RIP packet, it must decide whether or not to incorporate the route contained into its dynamic table. This is done as follows:

- The route is incorporated if it is not yet listed in the table (as long as there is enough space in the table).
- The route exists in the table with a time of '5' or '6'. The new route is then used if it indicates the same or a better distance.
- The route exists in the table with a time of '7' to '10' and thus has the distance '16'. The new route will always be used.
- The route exists in the table. The new route comes from the same router which notified this route, but has a worse distance than the previous entry. If a device notifies the degradation of its own static routing table in this way, the cable modem will take this into account and include the poorer entry in its dynamic table.

The interaction of static and dynamic tables

The router uses the static and dynamic tables to calculate the actual IP routing table it uses to determine the path for data packets. In doing so, it includes the routes from the dynamic table which it does not know itself or which indicate a shorter distance than its own (static) route with the routes from its own static table.

Local routing

You know the following behavior of a workstation within a local network: The computer searches for a router to assist with transmitting a data packet to an IP address which is not on its own LAN. This router is usually notified to the operating system by its property of being the default router or gateway. It is often only possible to enter one default router which is supposed to be able to reach all the IP addresses which are unknown to the workstation computer if there are several routers in a network. Occasionally, however, this default router cannot reach the destination network itself but does know another router which can find this destination.

How else can you assist the workstation computer?

By default, the router sends the computer a response with the address of the router which knows the route to the destination network (this response is known as an ICMP redirect). The workstation computer then accepts this address and sends the data packet straight to the other router.

Certain computers, however, do not know how to handle ICMP redirects. To ensure that the data packets reach their destination anyway, use local routing (in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Router' tab or in the `/Setup/IP Router`

Module/Local Routing On menu). This tells the router in your device to send the data packet to the other responsible router. The router will then no longer send any ICMP redirects.

This may seem to be a good idea in principle, but local routing should still only be used as a last resort, since this function leads to doubling of the number of data packets being sent to the destination network required. The data is first sent to the default router and is then sent on from there to the router in the local net which is actually responsible.

IP masquerading (NAT, PAT)

One continually growing problem for the Internet is the limited number of generally valid IP addresses available. In addition to this, the allocation of fixed IP addresses for the Internet by the Network Information Center (NIC) is an expensive process. What is more obvious than having several computers share one IP address?

This particular solution is called IP masquerading. This is a procedure whereby only one LAN router appears on the Internet with an IP address. This IP address is allocated to the router either permanently by the NIC or temporarily by an Internet provider. All the other computers on the network then “conceal” themselves behind this one IP address. Aside from the welcome savings, IP masquerading has the added benefit of guarding very effectively against attacks on the local network from the Internet.



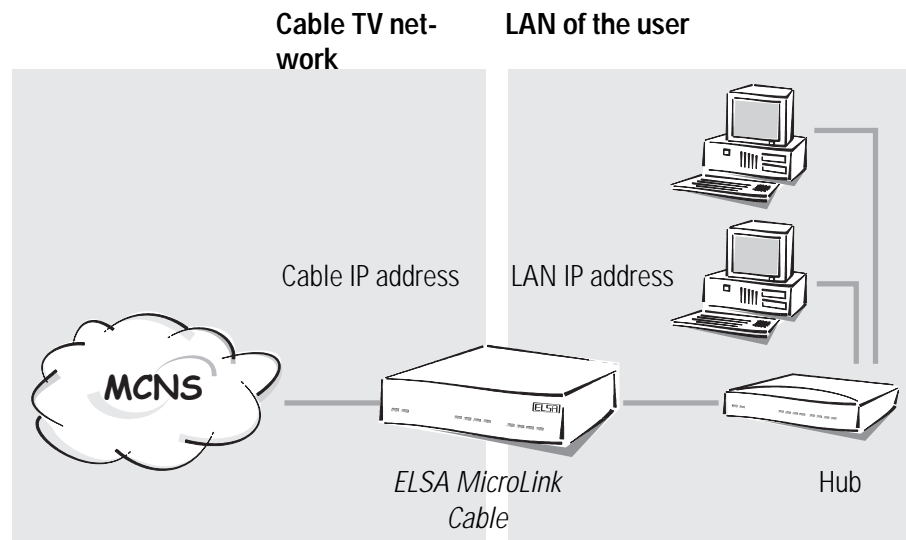
The IP masquerading function is connected to the operating mode of the cable modem as a router. Whenever routers are mentioned in the following paragraphs, this is a reference to the cable modem in the operating mode of an IP router.

Two addresses for the router

Masquerading pits two opposing requirements of the router against one another:

- On the one hand, it has to have a valid IP address in the local network of the user so that it can be reached from the LAN.
- On the other hand, it has to have a valid address in the cable network.

Since these two addresses may not in principle be located on the same logical network, there is only one solution: two IP addresses are required.



The cable modem is therefore assigned a cable IP address and a LAN IP address, each with its own appropriate network mask. Use the 'Masquerade' option to inform the cable modem which of the two addresses to use when transferring the packets.

- 'Off': No masquerading.
- 'on': Use this entry to apply the cable IP address that was assigned during the registration at the headend by the network operator.



If the cable modem is used as an IP router without masquerading, make sure that IP/RIP is enabled. When using it as an IP router with masquerading, IP/RIP should be disabled.

How does IP masquerading work?

Masquerading makes use of a characteristic of TCP/IP data transmission, which is to use port numbers for destination and source as well as the source and destination addresses. When the router receives a data packet for transfer it now notes the IP address and the sender's port in an internal table. It then gives the packet its unique cable IP address and a random new port number. It also enters this new port on the table and forwards the packet with the new information.

The response to this new packet is now sent to the cable IP address of the cable modem with the new sender port number. The entry in the internal table allows the router to assign this response to the original sender again.

You can view these tables in detail in the router statistics (see also 'Status').



Simple and inverse masquerading

This masking operates in both directions: The local network behind the cable IP address of the router is masked if a computer from the LAN of the user sends a packet to the Internet (simple masquerading).

If, on the other hand, a computer sends a packet from the Internet to, for example, an FTP server on the LAN, from the point of view of this computer the router appears to be the

FTP server. The router knows the IP address of the FTP server in the LAN from the entry in the service table (in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Masq.' tab or in the *Setup/IP Router Module/Masquerading/Service Table* menu). The packet is forwarded to this computer. All packets that come from the FTP server in the local network (answers from the server) are hidden behind the IP address of the router.

The only small difference is that:

- Access to a service (port) in the user's LAN from outside must be defined in advance by specifying a port number. The destination port is specified with the LAN IP address of, for example, the FTP server, on a service table to achieve this.
- When accessing the Internet from the LAN, on the other hand, the router itself makes the entry in the port and IP address information table.

The table concerned can hold up to 2048 entries, that is it allows 2048 **simultaneous** transmissions between the masked and the unmasked network.

After a specified period of time, the router, however, assumes that the entry is no longer required and deletes it automatically from the table.

Which protocols can be transmitted using IP masquerading?

Naturally, only those which also communicate using ports. Protocols working without port numbers or using ports above IP in the OSI model cannot be masked without special treatment.

The current version of router implements masquerading for the following protocols:

- TCP (and all TCP-based protocols such as FTP, HTTP etc.)
- UDP
- ICMP

DNS forwarding

Names rather than IP addresses are generally used to access a server over the Internet. Who knows which address is behind 'www.domain.com'? The DNS server, of course.

DNS stands for Domain Name Service refers to the assignment of domain names (such as domain.com) to the corresponding IP addresses. This information must be constantly updated and be accessible all over the world at any time. DNS servers holding long tables containing IP addresses and domain names exist for this purpose.

If a computer calls up a home page from the intranet, it first sends out a DNS request: "What is the IP address associated with www.domain.com?"

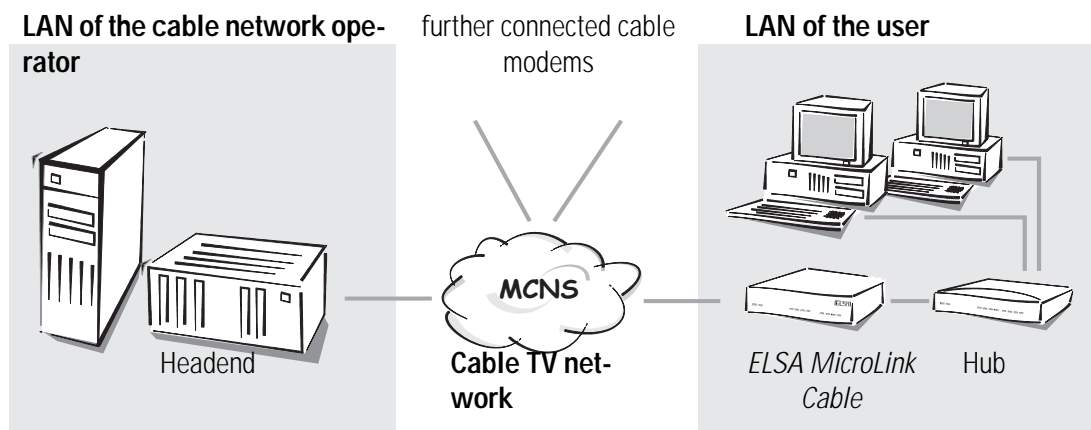
This request is dealt with as follows if the cable modem is registered as the DNS server for the workstation computers:

- Initially the router checks whether a DNS server has been entered in its own settings (in configuration tool *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Addresses' tab or in the /Setup/TCP-IP Module menu). If it finds it there, it will then retrieve the desired information from this server.
- If no DNS server has been entered in the cable modem, it tries to reach the network operator's DNS server to retrieve the IP address associated with the name. The address of the DNS at the network operator is transferred during the registration of the cable modem by the headend.

This procedure does not require you to have any knowledge of the DNS server address. Entering the LAN IP address of the cable modem as the DNS server for the workstation computers is sufficient to enable name associations. This procedure also automatically updates the address of the DNS server. Your local network always receives the most current information even if, for example, the provider sending the address changes the name of his DNS server or you change to another provider.

Bridging

A bridge connects two or more LANs in such a way that they appear to be a single large network. When bridging via cable modems, the LAN of the cable network operator with the headend is on one side and the LAN of the network participants with the cable modem and the local workstations on the other.



In the bridge operating mode, the *ELSA MicroLink Cable* transfers all data to computers without locally assigned MAC addresses, between the local network or another local area network (LAN) or a workstation on one side and the cable network on the other side.

The bridge thus learns on its own which MAC addresses are located on its own network and which are located on the other side. After a very high level of data traffic that occurs during the initial negotiations between the two LANs, the network load drops sharply. When receiving data from the cable network, the bridge in the cable modem uses the MAC addresses to determine whether the data is destined for its own LAN. The bridge will only accept data packets that are addressed to MAC addresses in its LAN.

What are the filter options?

You may not always wish to transfer all data. Much of the data which is bouncing around in the LAN is of no interest to remote networks or computers. You can thus block transfer of the following data packets via the bridge:

- Broadcast packets: Data directed at all devices accessible in a network (Setup/Bridge-Module/LAN-config/Broadcast).
- Multicast packets: Data which is transferred to all devices accessible in a group (Setup/Bridge-Module/LAN-config/Multicast).

Special filter lists which exclude certain addresses from a transmission or only allow certain addresses can be set up to handle this data. The bridge filters differentiate here between destination and source addresses. You can first establish for both address types whether the associated table contains the addresses to which data is to be transmitted (Setup/Bridge-Module/LAN-config/Dest.-address/Filter-type/pos) or the addresses to be excluded (.../Filter-type/neg). You then enter the MAC addresses to be filtered into the table itself.



This method of filtering by entering the exact MAC address naturally demands a certain degree of maintenance effort. Should the addresses change, when a network adapter is changed for example, the new addresses must be entered to ensure that the bridge continues to function.

Automatic address administration with DHCP

In order to operate smoothly in a TCP/IP network, all the devices in a local network must have unique IP addresses.

In addition to the IP addresses, the devices in the LAN also need the addresses of DNSs as well as that of a default gateway through which the data packets are to be routed from addresses that are not available locally.

In a smaller network, it is still conceivable that these addresses could be entered manually in all the computers in the network. In a larger network with many workstation computers, however, this would simply be too enormous of a task.

In such situations, the DHCP (Dynamic Host Configuration Protocol) is the ideal solution. Using this protocol, a DHCP server in a TCP/IP-based LAN can dynamically assign the necessary addresses to the individual stations.

The cable modem really belongs to two LANs:

- On one side it is a part of the LAN of the cable network operator and forms a LAN together with the headend and all connected cable modems. The cable network operator assigns the IP addresses to the participants via DHCP.
- On the other side the cable modem forms a separate LAN with one or more connected computers. DHCP can also be used to manage addresses within your own LAN.

The cable modem thus functions as a DHCP client and as a DHCP server.



Whenever IP addresses of the cable modem are mentioned in the following paragraphs, this is a reference to the LAN IP address of the ELSA MicroLink Cable, unless something else is explicitly stated.

The DHCP client

The cable IP address for the exchange of data in the cable network is assigned via DHCP by the network operator during registration at the headend, i.e. the network participant has no influence on this process. Apart from the IP address used by the cable modem when active on the cable network, additional information is transmitted such as the cable network operator's gateway into the Internet or the time server.

Since this assignment via DHCP from the cable network to the cable modem is mandatory, it is not necessary to configure the DHCP client. Current assignments can be read at any time in the `Status/DHCP client status` menu.

The DHCP server

As a DHCP server, the *ELSA MicroLink Cable* can manage the IP addresses in its TCP/IP network. In doing so, it passes the following parameters to the workstation computers:

- IP address
- Network mask
- Broadcast address
- DNS
- NBNS
- Default gateway
- Period of validity for the parameters assigned

The DHCP server takes the IP addresses either from a freely defined address pool or determines the addresses automatically from its own LAN IP address.

DHCP – 'on', 'off' or 'auto'?

The DHCP server in the devices of ELSA can be set to three different states:

- 'on': The DHCP server is permanently active. The configuration of the server (validity of the address pool) is checked when this value is entered.
 - When correctly configured, the device will be available to the network as a DHCP server.
 - In the event of an incorrect configuration (e.g. invalid pool limits), the DHCP server is disabled and switches to the 'off' state.
- 'off': The DHCP server is permanently disabled.
- 'auto': The server is in automode. In this mode, after switching it on, the device looks for other DHCP server within the local network.
 - The device then disables its own DHCP server if any other DHCP servers are found. This prevents the unconfigured router from assigning addresses not in the local network when switched on.
 - The device then enables its own DHCP server if on other DHCP servers are found.

Whether the server is active or not can be seen in the DHCP statistics.

The default state is 'auto'.

How are the addresses assigned?

IP address assignment

Before the DHCP server can assign IP addresses to the computers in the network, it first needs to know which addresses are available for assignment. Three options exist for determining the available selection of addresses:

- The IP address can be taken from the address pool selected (start address pool to end address pool). Any valid addresses in the local network can be entered here.
- If '0.0.0.0' is entered instead, the DHCP server automatically determines the addresses (start or end) from the LAN IP address settings in the 'TCP/IP module'.
- If the cable modem has no LAN IP address of its own, the device will go into a special operating mode. It then uses the IP address '10.0.0.254' for itself and the address pool '10.x.x.x' for the assignment of IP addresses in the network. In this state, the DHCP server only assigns IP addresses and their validity to the computers in the network, but not the other information.

If only one computer in the network is booted and requests an IP address via DHCP with its network settings, a device with an activated DHCP module will assign this computer an address. A valid address is taken from the pool as an IP address. If the computer was already assigned an IP address at some point in the past, it requests this same address

and the DHCP server attempts to reassign it this address if it has not already been assigned to another computer.

The DHCP server also checks whether the address selected is still available in the local network. As soon as the uniqueness of an address has been established, the requesting computer is assigned the address found.

Network mask assignment

The network mask is assigned in the same way as the address. If a network mask is entered in the DHCP module, this mask is used for the assignment. Otherwise, the network mask from the TCP/IP module is used.

Broadcast address assignment

Normally, an address yielded from the valid IP addresses and the network mask is used for broadcast packets in the local network. In special cases, however (e.g. when using subnetworks for some of the workstation computers), it may be necessary to use a different broadcast address. In this case, the broadcast address to be used is entered in the DHCP module.



The default setting for the broadcast address should be changed by experienced network specialists only.

DNS server assignment

The addresses of the DNS servers are negotiated and entered during the registration at the headend.

Default gateway assignment

The router always assigns the requesting computer its own IP address as a gateway address.

If necessary, this assignment can be overwritten with the settings on the workstation computer.

Period of validity for an assignment

The addresses assigned to the computer are valid only for a limited period of time. Once this period of validity has expired, the computer can no longer use these addresses. In order for the computer to keep from constantly losing its addresses (above all its IP address), it applies for an extension ahead of time that it is generally sure to be granted. The computer loses its address only if it is switched off when the period of validity expires.

For each request, a host can ask for a specific period of validity. However, a DHCP server can also assign the host a period of validity that differs from what it requested. The DHCP module provides two settings for influencing the period of validity:

■ **Maximum lease time in minutes**

Here you can enter the maximum period of validity that the DHCP server assigns a host.

If a host requests a validity in excess of 6000 minutes, this will nevertheless be the maximum available validity!

The default setting is 6000 minutes (approx. 4 days).

■ **Default lease time in minutes**

Here you can enter the period of validity that is assigned if the host makes no request. The default setting is 500 minutes (approx. 8 hours).

Priority for the DHCP server – Request assignment

In the default configuration, almost all the settings in the Windows network environment are selected in such a way that the necessary parameters are requested via DHCP. Check the settings by clicking **Start ► Settings ► Control Panel ► Network**. Select the 'TCP/IP' entry for your network adapter and open **Properties**.

Check the various tabs for special entries, such as for the IP address or the standard gateway. If you would like all of the values to be assigned by the DHCP server, simply delete the corresponding entries.

Priority for a workstation—overwriting an assignment

If a computer uses parameters other than those assigned to it (e.g. a different default gateway), these parameters must be set directly on the workstation computer. The computer then ignores the corresponding parameters assigned to it by the DHCP server.

Under Windows, this can, for example, be performed via the properties of the network environment.

Click **Start ► Settings ► Control Panel ► Network**. Select the 'TCP/IP' entry for your network adapter and open **Properties**.

You can now enter the desired values by selecting the various tabs.

The assignment of IP addresses to the various computers can be checked using the 'Setup/DHCP/Table-DHCP' item in the router's DHCP module. This table contains the assigned IP address, the MAC address, the validity, the name of the computer (if available) and the type of address assignment.

The 'Type' field specifies how the address was assigned. This field can assume the following values:

- new

The computer has made its initial request. The DHCP server verifies the uniqueness of the address that is to be assigned to the computer.

- unknown

While verifying uniqueness, it was determined that the address has already been assigned to another computer. Unfortunately, the DHCP server has no means of obtaining additional information on this computer.

- status

A computer has informed the DHCP server that it has a fixed IP address. This address can no longer be used.

- dynamic

The DHCP server assigned an address to the computer.

Technical basics

This chapter is a short introduction into the technology used by your device. Network professionals will find themselves just skimming these pages, but novices will find this section to be very helpful for understanding the technical terms and processes.

Cable modem technology

The cable modem belongs to a new, promising generation of Internet access technology. This device differs from conventional analog and ISDN modems in that it communicates via the broadband radio and cable TV available in nearly all households, rather than the usual telephone lines.

Downstream:
*Transfer of data
from the
provider to the
Internet user*

This cable is well-suited for the transfer of large volumes of data. Up to now, the one-way flow of data from the provider to the user (downstream) has been a problem for such applications, however. Videotext uses this downstream data transfer: the provider, in this case the television broadcaster, continuously transmits a selection of information in the form of individual pages over the cable network.

Upstream:
*Transfer of data
from the
Internet user to
the provider*

The user can then choose a page, by entering a number for example. However, the user is restricted to the broadcaster's selection and cannot send data back (upstream).

Standards

Two standards get around this problem:

- The first solution accepts the restriction of the cable network to downstream transfers and handles the upstream using normal telephone lines. The disadvantage is obvious: it requires an additional line on the telephone network (through a normal modem, for example) subject to telephone connect charges.
- A standard that was successfully applied in the USA equips the cable network with suitable amplifiers and remote stations for the transfer of data back to the provider. These remote stations are called headends or CMTSS (**C**able **M**odem **T**ermination **S**ystem). Connections using the MCNS standard (**M**ultimedia **C**able **N**etwork **S**ystem) no longer need an extra telephone connection. Access to the Internet is thus no longer subject to time-related connect charges, in effect providing the user with a permanent connection to the Internet.

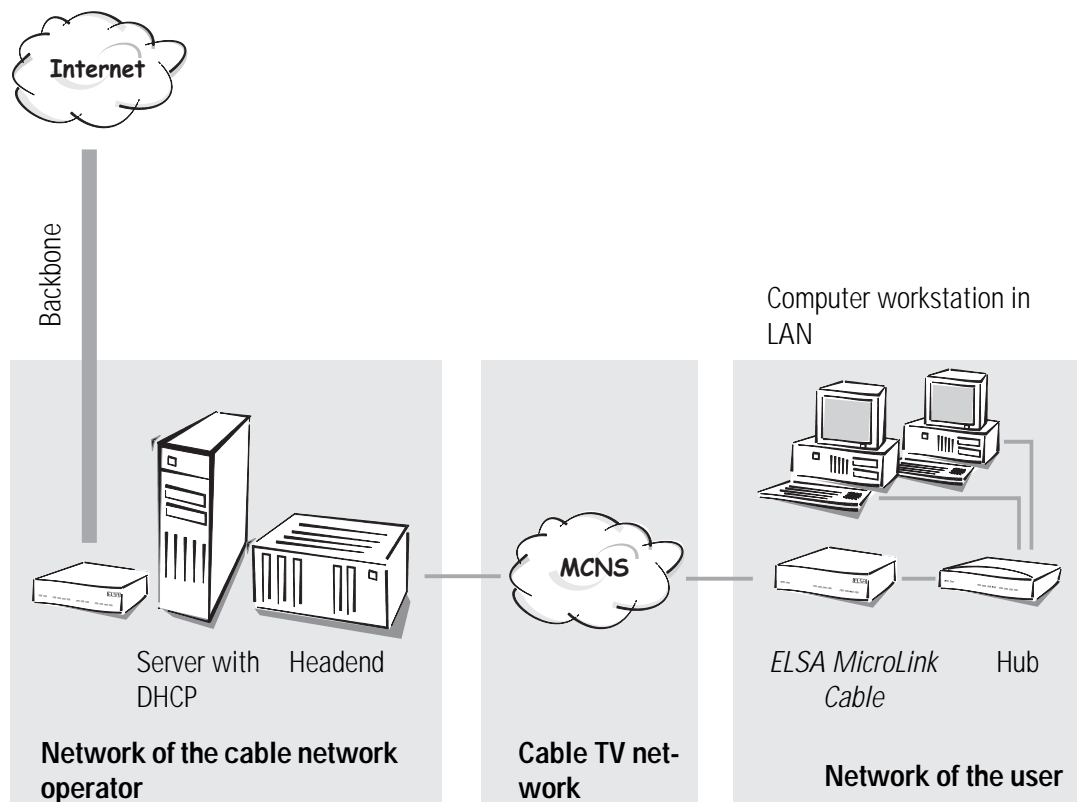
Access

To clarify access to the Internet through the cable network (using a simplified description), let's have a look at both sides of the connection. On one side we have the user, who would like to connect to the Internet with a local network or an individual

computer. On the other side is the operator of the broadband cable network who would like to provide more than just radio and TV.

A headend can accommodate up to 2000 individual users with cable modems like the *ELSA MicroLink Cable*. The headend functions as a multiport, however, giving every user access to the cable network at any time. Unlike access through analog or ISDN modems, there are no connection attempts that could fail because all of the provider's ports are already in use. No further hardware is needed for the connection between the Internet user and the network operator as long as both the cable modem and the headend use the bidirectional MCNS standard.

On the other side, the network operator has to establish a connection to the Internet. He can either act as an Internet service provider (ISP) himself and directly establish access to the Internet, or he can outsource this task on to another ISP or an online service.



This connection to the backbone is of little relevance to the user. However, the greater the performance of the network operator's backbone line, the quicker the users receive information from the Internet.

Registration in the cable network

In comparison to other data transfer media, the cable TV network has a very high bandwidth at its disposal—thus the term broadband cable network. The full bandwidth is divided up into a variety of channels that are reserved for the transmission of different kinds of information. You know this from television, where you also find different

programs on their respective channels. Specific channels are also set up for the transmission of Internet content.

Synchronizing

Finding a channel in the broadband network

After being switched on, the cable modem searches the entire frequency band for a channel used by the provider to send information from the Internet. Because the bandwidth is so great, the first time the log-on procedure might take a while. As soon as the corresponding channel is found, the Sync LED on the *ELSA MicroLink Cable* flashes. The next time the cable modem is switched on, it will first look for the channel it found the previous time, and thus find the wanted information at a substantially faster rate. However, if the cable modem is used on another connection, it may have to search the entire frequency band again.

To speed up the search, providers can preset the *ELSA MicroLink Cable* to search the particular frequency bands that they normally use.



Do not change these settings yourself without consulting your provider.

Registration

Exchange of administration information between head-end and cable modem

When a channel for communication with the provider has been found, the headend gives a set of instructions to the cable modem that is important to the operation in the cable network. This process is called registration. It includes:

- The confirmation of the found channel or the transfer to another channel
- The allocation of an IP address that is valid in the cable network, along with a suitable netmask
- Information on the provider's server addresses
- The current time

After the registration is completed successfully, the Reg'd LED on the *ELSA MicroLink Cable* lights up and the cable modem is ready to access the Internet.

Network technology



*This section will give you a brief introduction to the basics of network technology. These descriptions do **not** cover all possible techniques, processes and terms associated with network technology. They only cover the topic to the degree necessary to provide an understanding of the product information.*

The network and its components

*Network,
transmission
medium,
interfaces*

Whenever several computers communicate with one another, this connection is called a network. For computers to be able to communicate, they need a physical medium through which the information can be transmitted. This can be a cable or radio link, for example, that is connected to the computers using special interfaces (e.g. network adapters).



*Packets
Cells*

The term network cable (or simply cable) in the following text also refers to any other physical medium that can take on the function of the cable, such as wireless links.

The individual bits of electronic information that are sent from one computer to another through a medium are called packets or cells, depending on the process.



For most of the following explanations, the difference between packets and cells is irrelevant. Therefore, we will use the term packet or data packet in a general sense and only detail the special characteristics of cells as necessary.

Host

The computer and other terminal devices (e.g. the printer) in a network that generate or process information are called hosts. Ideally, a host is not responsible for the task of forwarding information. A host normally has exactly one interface to the network.

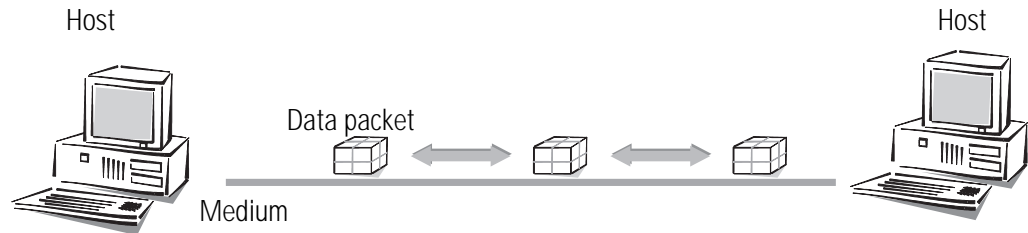
Router

The transport of packets between two hosts occurs indirectly through exchanges that pass packets on to the target computer. These exchanges are called routers. A router has at least two interfaces so that it can receive the data from a sender and pass them on to a recipient. Apart from the exchange function, the router also has the properties of a host so that it can also be the recipient of data packets, for configuration purposes for example.

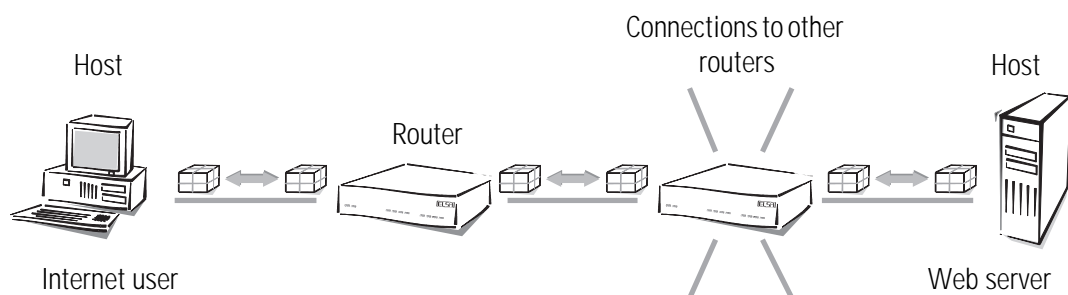
Connection modes

*Point-to-point
connection*

The connection of exactly two hosts via a medium is called a “point-to-point connection”. In this case a host sends packets that can only be received by **one** specific recipient (unambiguous connection).



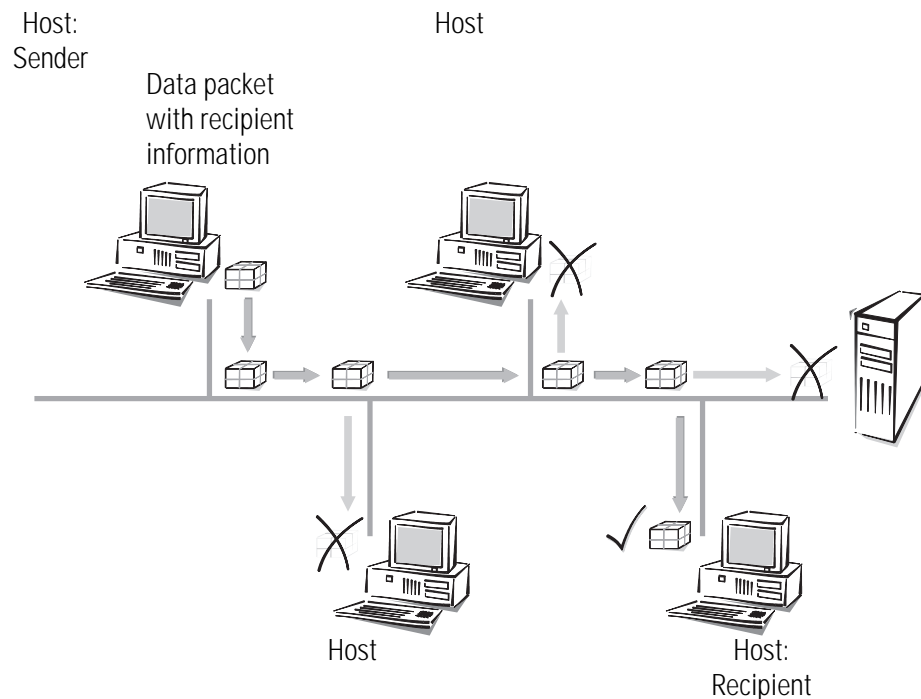
Access to the Internet is also established through point-to-point connections. Even though the data packets are sent from the host at the Internet user to the host at the Internet provider (server) via several routers, every data packet still has its own specific destination. Furthermore, the routers will only forward the data packets to one recipient. That's why we also call this connection unambiguous.



Strictly speaking, the term “point-to-point connection” is not quite correct. For our purposes though, it is sufficient to distinguish this kind of connection from the following “point-to-multipoint connections”.

Point-to-multipoint connection

Generally speaking, it would be uneconomical to directly connect all computers in a network via point-to-point connection cables, as the computers would then require multiple interfaces. Computers in a network are therefore plugged into a joint medium shared by all hosts. The sender simply sends its packet with instructions concerning the recipient to the medium to which other hosts are connected. The data packet arrives at **every** host in the network. Each host then decides whether it is the recipient of the packet or not. If the packet is addressed to the corresponding host, it will then accept it. If not, the host will ignore (reject) it. This is a “point-to-multipoint connection”, since we are not dealing with an unambiguous connection.



Kinds of networks

<i>Protocol</i>	An important prerequisite for communications between computers is a common language among the hosts. In the world of network technology this language is called "network protocol" or simply "protocol".
<i>TCP/IP</i>	The most broadly distributed network protocol is the TCP/IP (T ransmission C ontrol P rotocol/ I nternet P rotocol). It is used mainly in the Internet, but nowadays more and more company networks use it. Examples of other network protocols are IPX or Apple Talk. Because of its wide use, this chapter deals mainly with the TCP/IP.
<i>IP network</i>	All hosts wanting to communicate using the TCP/IP protocol have to be plugged into the same network and have to have the TCP/IP protocol (also known as TCP/IP stack) installed. Such a network is referred to as an IP network.
<i>Internetwork Internet</i>	The connection of multiple networks based on the IP protocol is referred to as an internetwork. The largest union of many small, public IP networks is the Internet.
<i>Local network (LAN)</i>	A network covering a limited area with hosts on the same hierarchical level and using the same medium (shared medium) is called a local network (L ocal A rea N etwork, LAN).

IP addressing

<i>Packet-oriented transfer</i>	In IP networks the communication between computers takes place in a packet-oriented fashion. This means that data or messages are packed together in packets of variable length and are as such sent from the source computer to the target computer. Apart from
---------------------------------	--

the actual information to be transmitted (useful data), the data packet also contains address and control information.

IP address

IP addresses are used in IP networks for communications between various devices. In this case, every host has its own unique address by which it can be identified unambiguously. What does an IP address look like? It consists of four bytes separated by dots, making a total of 32 bits. Each of the four bytes can take on values from 0 to 255, e.g. 192.168.130.124.



To be precise, the IP address refers to the interface, and not the host itself. A terminal device with more than one interface (such as a router) has to have an IP address at its disposal for every single interface. This is why ISDN routers from ELSA for example, have an IP address for communication with the hosts in their own network, as well as a second IP address for communication with the "outside world" using the ISDN. In the same way, ELSA cable modems have an IP address for their own network and another IP address for the exchange of data with the cable network.

Network address

An IP address contains the address of the network as well as that of the host. The network address is the same for all hosts on one network, whereas the address of the host is exclusive and unique to the network. A router, for example, can have more than one IP address, each one unique to the network.

Netmask

How then can you differentiate between the part that determines the network and the part that identifies the host? With the netmask. You know what masks are: they cover up one part of something and only allow a different part to be visible. This is exactly how a netmask operates. It is a number which is identical in structure to the IP address, i.e. 32 zeros or ones. The netmask usually starts with ones at the beginning and ends with zeros. The zeros at the end thus cover the part of the IP address which does not belong to the network address.

Examples:

This address...	...in bytes...	...looks like this in bits:
IP address	192.168.120.253	11000000.10101000.01111000.11111101
Netmask	255.255.255.0	11111111.11111111.11111111.00000000
Network address	192.168.120.0	11000000.10101000.01111000.00000000

The same IP address, this time with another netmask:

This address...	...in bytes...	...looks like this in bits:
IP address	192.168.120.253	11000000.10101000.01111000.11111101
Netmask	255.255.0.0	11111111.11111111.00000000.00000000
Network address	192.168.0.0	11000000.10101000.00000000.00000000

You can see from this that an IP address alone is not enough. A host can only be identified unambiguously in combination with a netmask.

And you can also see that there are more bits available to identify the individual hosts in a connected network if there are fewer bits in a netmask that contain a one. While only 254 different addresses could be allocated in the first example with the netmask 255.255.255.0, the second example has as many as $254 \times 254 = 64516$ different addresses available! The first and the last digit of an address space are reserved for the network address and the broadcast address (addresses for packets to all hosts in an IP network). In the netmask 255.255.255.0 this is the '0' for the network address and the '255' for the broadcast address.

A new notation of the netmask simply attaches the number of bits available for the network address to the IP address: 137.226.4.101/24. The number after the slash tells us that the first 24 bits indicate the network address. This notation reduces the length of the entries in the routing tables.

IP address management

The IP addresses must be unique within a specific network in order to avoid confusion. Since the Internet is based on TCP/IP and thus uses IP addresses for its millions of connected computers, all Internet addresses must also be unique. Bodies exist that manage and distribute these publicly-accessible addresses. Since the number of IP addresses theoretically available is limited, these distributing bodies charge high rates for the addresses.

Private address spaces

A range of IP addresses are reserved for use free of charge (private address spaces) so that companies do not have to purchase individual IP addresses for every workstation. In a closed network, these addresses can be used as desired, in a private network or company, for example. The same address can be used in other closed networks (e.g. in different companies), but the addresses within one network must be unique.

However, these reserved IP addresses must **not** be made public (on the Internet). Only **those** devices in a network that are connected to a public network (e.g. the router at the interface to the Internet) must have a registered IP address.

The allocation of IP addresses by the IANA (Internet **A**ssigned **N**umbers **A**uthority) permits the following address ranges to be used for private use:

IP address	Netmask	Remark
10.0.0.0	255.0.0.0	"10" networks: All IP addresses beginning with 10. and whose mask begins with 255. belong to the address range reserved for private use.
172.16.0.0	255.240.0.0	All IP addresses beginning with 172.16.–172.31. which are associated with a net mask greater than or equal to 255.240.0.0 are within the address range reserved for private networks.
192.168.0.0	255.255.0.0	All IP addresses beginning with 192.168. and whose mask begins with 255.255. belong to the address range reserved for private use.
224.0.0.0	224.0.0.0	All IP addresses beginning with a 224 which are associated with a net mask also beginning with 224 are within the reserved address range. This range is reserved for broadcasting purposes and should not be used for private networks.

There are two considerations when using these IP addresses:

- The IP addresses used in a private network should not leave this network, i.e. an Internet connection is only possible when using IP masquerading, for example.
- The packets for these IP addresses will not be routed in the Internet, i.e. backbone routers will simply reject such IP packets. Depending on the provider, serious consequences may result if such IP packets are released on the Internet.

IP routing and hierarchical IP addressing

Routing

Every IP packet contains the IP addresses of the source and of the recipient. A router receives IP packets at its interface, interprets the destination address and passes the packets on to those interfaces that are nearest to the recipient. Finding the appropriate path is called routing.

Routing-table

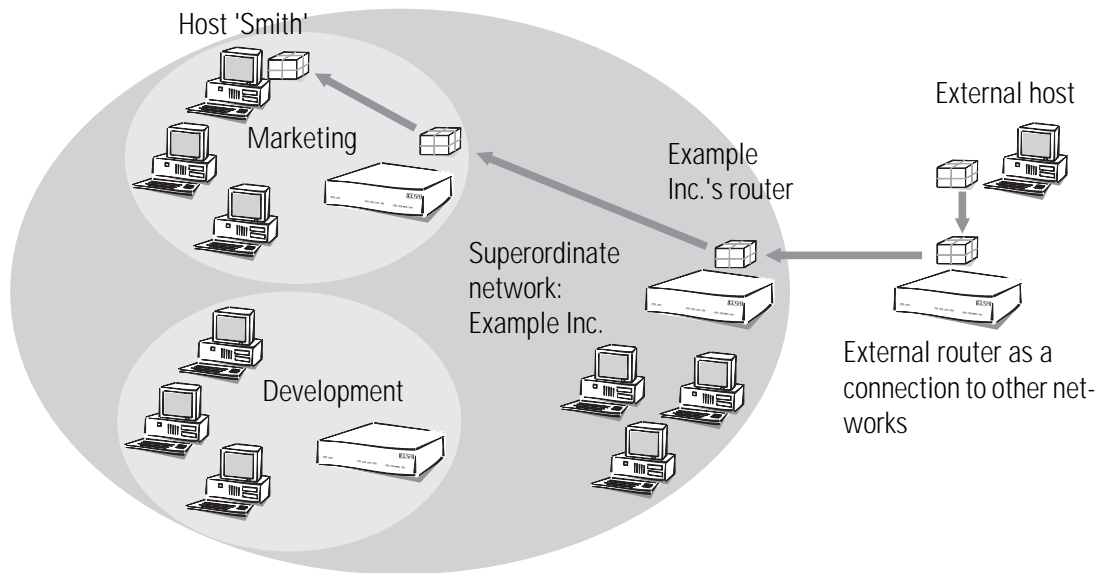
Every router manages a table (routing table). This table indicates the quickest interface connection to the host for every host in the network. You can imagine that, as they grow, these tables may exceed the capacity of the router—the Internet, as a worldwide linking up of publicly accessible IP computers contains several millions of hosts.

Hierarchical IP addresses

For this reason, hierarchical IP addresses were introduced. This means dividing the IP network into subnets in which IP addresses are appointed from a coherent numerical range. It is possible to establish several hierarchy levels, so that different subnets can be merged. The principle is similar to the hierarchical address used by paper mail, consisting of a country, a city, a street and a number.

The consequences of this hierarchical IP addressing:

- Since all hosts within one network have the same network address, the host address is sufficient for the hosts within this network to communicate with one another.
- A router has to know both the addresses of the hosts that are directly connected to it, and the addresses of all networks and subnets that are reachable via adjacent routers.
- It is **not** necessary for a router to know **all** other possible IP addresses.



As an example, think of a company with one large network, in which the different divisions are incorporated as small subnets. The address of the network for the marketing division is made up hierarchically from the address of the company and that of the department.

Whenever a host external to the company network sends a packet to a host in the Example Inc., this is what happens:

- ① The sender gives the packet the destination address "host 'Smith' – Marketing – Example Inc.".
- ② All an external router that establishes the connections to other networks has to know is how to reach Example Inc. As soon as it receives a packet with the address for Example Inc., it passes the packet on to the router responsible for Example Inc.
- ③ The router at Example Inc. receives the packet and extracts from the address the information that it is directed at Example Inc. Since it is itself part of Example Inc., it takes a closer look at the address to find the name of the division. It then passes the packet on to the router in the marketing division.
- ④ The router in the marketing division receives the packet and extracts from the address the information that it is directed at the marketing division of Example Inc. Since it is itself part of this division, it takes a closer look at the address to find the name of the host. It then passes the packet on to the host of the employee Sam 'Smith'.

Now we shall take a look at the example using proper IP addresses instead of symbolic names. The network of Example Inc. has the numerical space '192.168.100.0' to '192.168.100.255' at its disposal, with the '0' for the network address and the '255' for the sender address.

All the router has to remember is that every address beginning with '192.168.100' is located within the network of Example Inc.

Now imagine a router that is connected to the network of Example Inc. through an interface. If it receives a packet with destination address '192.168.100.4' and netmask '255.255.255.0', it will compare this with every network address it knows. In doing so it carries out a logical AND with the netmask, and compares the results with the network address: '192.168.100.4' AND '255.255.255.0' is '192.168.100.0'. This is the network address of the Example Inc. network. The router recognizes that the recipient is located within Example Inc. and passes the packet on to the appropriate interface for Example Inc. Within Example Inc. the packet is then passed on to the appropriate subnet.

The same procedure is used for the transfer of IP packets within a network:

- ① If a host in the subnet of the development department wants to send a data packet to Mr. 'Smith', the sender attaches the destination address "Host 'Smith' – Marketing – Example Inc.".
- ② The router in the development division receives the packet and extracts from the address the information that it is directed at the marketing division of Example Inc. Since it is itself part of Example Inc., but not of the marketing division, it passes the packet on to the router in the superordinate network.
- ③ The router at the Example Inc. receives the packet and extracts from the address the information that it is directed at Example Inc. Since it is itself part of Example Inc., it takes a closer look at the address to find the name of the division. It then passes the packet on to the router in the marketing division, where the packet is passed on to the recipient.

Expansion through local networks

Media access control

Up to now we have only considered the point-to-point connections. However, many computer networks are based on multipoint cabling such as Ethernet. All computers connected to the same network can then receive the signals of all other computers (so-called broadcast transfer to a shared medium). If several computers are sending simultaneously, the superimposed signals are destroyed. A variety of access methods such as CSMA/CD or Token Ring are implemented in the MAC layer (**M**edia **A**ccess **C**ontrol, MAC) for the avoidance and resolution of such collisions.

LAN and IP network

The connection of all computers communicating through a shared medium using a MAC protocol is called a LAN. A LAN forms an independent network and is subordinate to the IP network, i.e. IP networks can use the physical connections of the LAN to establish connections between the hosts and the routers. LAN refers to a limitation of the area covered by the network, not a restriction of the number of workstations connected to it.

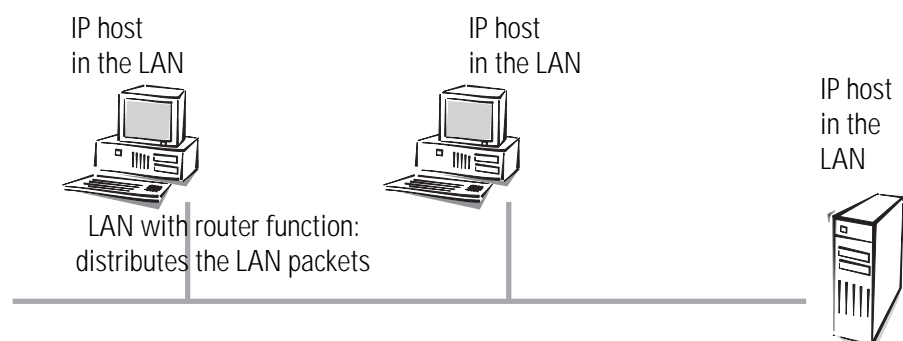
MAC address Specific LAN addresses hardwired into the interfaces by their manufacturers are used to manage the transfer in the LAN. Since the LAN addresses are used for communication via the MAC protocol, they are called MAC addresses. They can be thought of as the fingerprint of the interface hardware. MAC addresses can look like this, for example: 00-80-C7-6D-A4-6E.

MAC addresses are independent of IP addresses. An IP host whose interface works through a LAN has an IP and a MAC address. Whereas the structure of IP addresses with its similarity to postal addresses is supposed to simplify routing in enormous IP networks, the fingerprint-like MAC addresses are designed to make the connection to a LAN as easy as possible.

Transfer in LAN is also packet-oriented. Every MAC packet contains the MAC addresses of the source and of the recipient. Although every packet is received by all computers, it is processed only by the target computer. There is an additional MAC broadcast address that is processed by all computers in the LAN.

IP in the LAN Every LAN packet contains an entry with the type of the network protocol. An IP packet can be transferred through a LAN by packing it in a LAN packet and adding the 'IP' protocol type to it. Because of the IP entry, the LAN interface at the receiving host recognizes that the LAN packet contains an IP packet, extracts it and processes it as an ordinary IP packet. In this way, IP packets and packets of other network protocols like IPX can be transferred simultaneously through the same LAN without conflicts (this is why a LAN is called multiprotocol-capable).

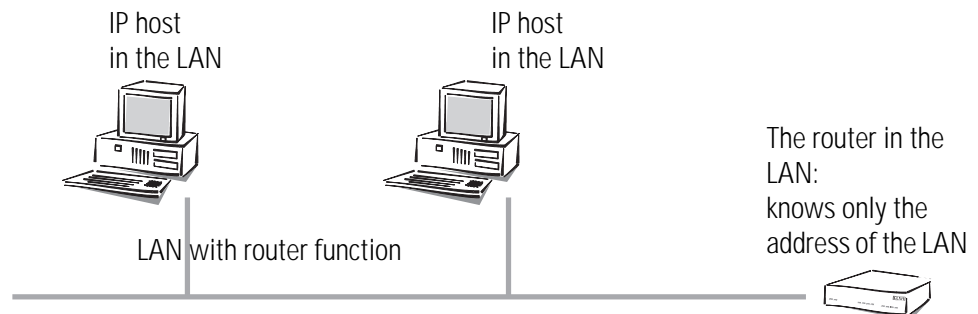
To an IP host, a LAN behaves as if it were an independent network with a router. The hosts gives the packets to the LAN which handles the further distribution of the data packets. This is why only IP addresses from the numerical space of the specific network should be used for the internal communication of the hosts in a LAN through the IP protocol.



To a router in the LAN, a host in its own LAN seems to be located behind another router. So the task for the router is very simple: all it has to know for operating in the IP network are the IP addresses

- of the directly connected hosts and
- of the available networks and subnets,

i.e. all it has to remember is the network address and the netmask of the subnet in the LAN.



In contrast, the host is confronted with a more difficult task than the router. In case of an interface with a point-to-point cable, the host knows that all packets that it sends through the interface automatically arrive at its router, for example. In case of the point-to-multipoint connection to the LAN, it has to distinguish two cases, however.

- A packet with an address outside the LAN is passed on to a router in the LAN that takes care of the further processing of the packet.
- The sending host must send a packet with an address within the LAN directly to the target host, since the router in the network does not know the addresses of all the different hosts.

Data transfer within the LAN

Let's use an example to explain this. Imagine the hosts of the subnet in the marketing division are linked via a LAN. The hosts have IP addresses from the numerical space '137.226.4.1' to '137.226.4.254' (the addresses '137.226.4.0' and '137.226.4.255' are reserved), the network address is '137.226.4.0' and the netmask is '255.255.255.0'. A router connected to the LAN provides access to the wide world of the Internet. Its LAN interface has the IP address '137.226.4.1' and the MAC address '00-80-C7-6D-A4-6E'.

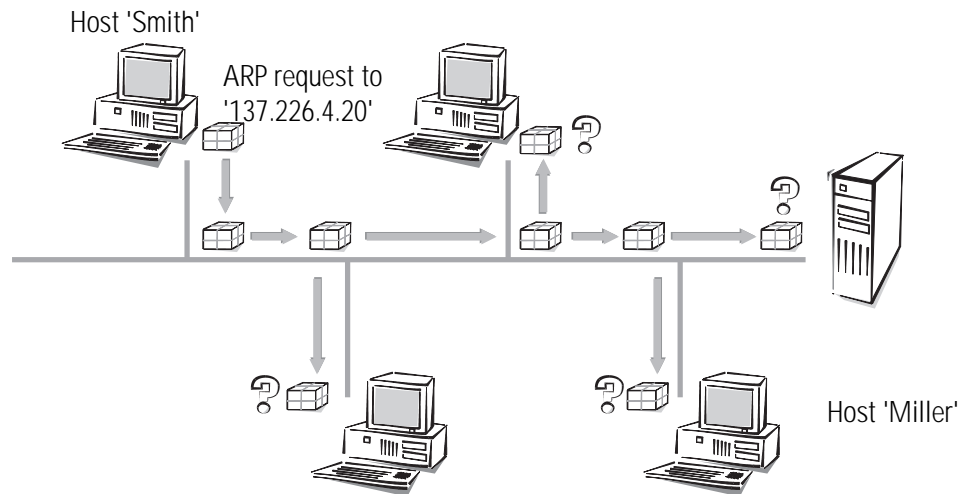
Imagine wanting to send an IP packet from host 'Smith' (with IP address '137.226.4.10' and MAC address '00-10-5A-31-20-DF') to host 'Miller' (with IP address '137.226.4.20' and MAC address '00-10-5A-31-20-EB'). Using the network address and the netmask, host 'Smith' recognizes that host 'Miller' is located in the own network. It therefore has to send the packet through the LAN, directly to host 'Miller'. Unfortunately the LAN interface cannot say: "Send the IP packet to IP address 137.226.4.20", because the LAN interface only understands MAC addresses.

This is why every host has to manage a table that translates IP addresses to MAC addresses. But how do the entries end up in the table? They could be entered manually, but that would not satisfy the objective of making the connection of a new computer to the LAN as easy as possible.

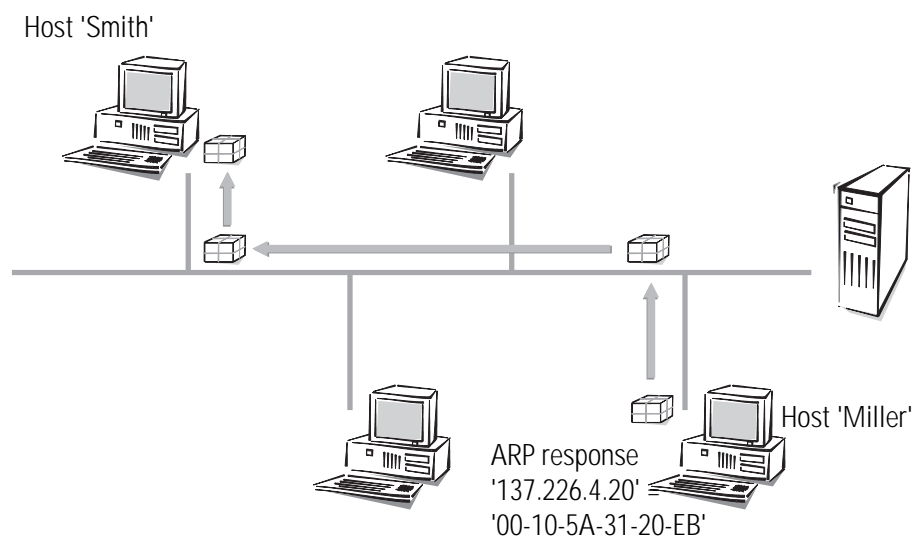
ARP

Therefore the LAN has a special mechanism that automates this process: the **Address Resolution Protocol**, ARP. The table itself is called the ARP table. Whenever a host does

not find an entry in the table for a particular IP address (in our example '137.226.4.20'), it sends an ARP request packet to all hosts in the LAN (with the LAN broadcast address as a target address).



This ARP request packet is simply a question to all hosts listening to the IP address '137.226.4.20'. Host 'Miller' receives the packet, feels addressed and answers with an ARP response packet that it sends directly to host 'Smith' (the MAC address '00-10-5A-31-20-DF' of host 'Smith' is extracted from the sender field in the ARP request packet). Host 'Smith' recognizes this as an answer to its request, extracts the MAC address '00-10-5A-31-20-EB' from the ARP response packet and enters it into its ARP table.



Then it can finally turn to its original task: sending the IP packet to host 'Miller'. It now finds the entry "IP address 137.226.4.20 corresponding to MAC address '00-10-5A-31-20-

EB'" in the ARP table and tells its LAN interface: "Send this IP packet to the computer with the MAC address '00-10-5A-31-20-EB'".

Data transfer from the LAN onto the Internet

Imagine the second task, sending an IP packet from host 'Smith' to the remote host 'External' with IP address 151.189.12.43. Host 'Smith' compares the IP address with its network address and realizes that host 'External' is located outside the LAN. So host 'External' can only be reached through the router. Host 'Smith' finds out the MAC address of the router '00-80-C7-6D-A4-6E' by looking up the router's IP address in the ARP table (if necessary another ARP request is made). So host 'Smith' tells its LAN interface: "Send this IP packet to the computer with the LAN address '00-80-C7-6D-A4-6E'". The router extracts the IP packet from the LAN packet and finds out about the IP address of host 'External'. In the routing table the router then looks for the network address of this host and thus finds the interface through which to pass on the IP packet.

LAN coupling on MAC basis

You know how LANs simplify the connection of computers to a local network. Nearly all house networks are thus LAN based. In some cases a LAN is covers such a large area that the physical characteristics of the cable prohibit the connection of any more computers. This results in the necessity to couple up several LANs in such a way that electrically and in terms of the MAC protocol they act as independent LANs, but for the IP protocol look like one big LAN.

This coupling of LANs is carried out using bridges. A bridge works somewhat like a router, but uses only MAC addresses for routing, not IP addresses. Since MAC addresses do not give any information on the structure of the network the way IP addresses do, every bridge has to know all MAC addresses in the entire LAN.

And so we encounter the same problem that we had with the routers before the introduction of subnets: As the LAN expands, it will at some point exceed the capacity of the address tables of the bridges. So one cannot use bridges to connect an infinite number of LANs. On the other hand, the unstructured MAC addresses allow the bridges to learn automatically about the location of computers in the network, using the received packets. This is called an "intelligent bridge".

Appendix

Technical data

Technical data	<i>ELSA MicroLink Cable</i>	
LAN interface	Ethernet IEEE 802.3, 10Base-T (Twisted Pair, RJ45, Node/Hub switch)	
Cable TV interface	MCNS DOCSIS (ITU-T J.112, physical layer as per Annex A & Annex B, MAC as per Annex B)	
	Socket:	F –socket (IEC169-2 connection via included adapter)
	Reception frequency band:	88 - 860 MHz
	Reception channel width:	6 MHz or 8 MHz
	Receiver level:	48 W – 78 dB μ V
	Receiver modulation:	64QAM, 256QAM
	Receiver data rate:	30.34 Mbps (64QAM), 42.88 Mbps (256QAM)
	S/N ratio in receive direction:	> 21 dB (64 QAM) > 28 dB (256 QAM)
	Transmission frequency band:	5 – 42 MHz (5 – 65 MHz optional)
	Transmission channel width:	200 – 3200 kHz
	Transmission level:	85 – 122 dB μ V
	Transmission modulation:	QPSK, 16QAM
	Transmission data rate:	0,32 – 5,12 Mbps (QPSK), 0,64 – 10,24 Mbps (16QAM)
	S/N ratio in transmit direction:	> 14 dB (Burst QPSK) > 20 dB (Burst 16QAM)
Network protocols	Bridge mode:	Bridging of all IEEE 802.3-based protocols
	IP router:	IP, TCP, ICMP, ARP, RIP-1, RIP-2, PROXY ARP, DHCP
Filter possibilities	Bridge mode:	Broadcast, multicast, destination MAC address, source MAC address, automatic filtering of local and remote stations
	IP router	TCP, UDP port filtering, source and destination network filter
IP masquerading (NAT/PAT)	Internet access using a single IP address via IP address and port implementation, static/dynamic IP address assignment via DHCP, masking of TCP, UDP, ICMP and FTP; DNS forwarding; inverse masquerading for intranet IP services	
Management	Cable network operator:	Via SNMP and TFTP (transfer of configuration files and firmware updates)
	User:	Via the cable TV network or LAN with TCP/IP, password protection, <i>ELSA LANconfig</i> , SNMP, TFTP, telnet
Display/operation	LEDs for LAN and cable TV network status, factory-default button, reset button	
Power supply	12 V AC with AC adapter for 230 V (US version: 110V), 10 VA	
Ambient conditions	Temperature: 5 - 40°C, humidity: 0 - 80%, non-condensing	
Dimensions and design	Rugged metal case, LEDs on front panel, connections on rear panel; Dimensions: 158 x 32 x 135 mm (W x H x D)	

Technical data	<i>ELSA MicroLink Cable</i>	
Package contents	Accessories:	AC adapter, F-to-IEC169-2 adapter, connector cable for cable TV network, 10Base-T cable
	Software:	Configurations software <i>ELSA LANconfig</i> , TFTP client
	Documentation:	Comprehensive manual and <i>ELSA</i> CD-ROM
	Installation Guide:	German, English, French, Italian, Dutch, Spanish
Service	Warranty:	6 years
	ELSAcare:	In the event of a warranty claim within the first 100 days following the purchase, replacement product will be provided.
	Support:	Via hotline and Internet

Warranty conditions

The ELSA AG warranty, valid as of June 01, 1998, is given to purchasers of ELSA products in addition to the warranty conditions provided by law and in accordance with the following conditions:

1 Warranty coverage

- a) The warranty covers the equipment delivered and all its parts. Parts will, at our sole discretion, be replaced or repaired free of charge if, despite proven proper handling and adherence to the operating instructions, these parts became defective due to fabrication and/or material defects. Also we reserve the right to replace the defective product by a successor product or repay the original purchase price to the buyer in exchange for the defective product. Operating manuals and any supplied software are excluded from the warranty.
- b) Material and service charges shall be covered by us, but not shipping and handling costs involved in transport from the buyer to the service station and/or to us.
- c) Replaced parts become property of ELSA.
- d) ELSA are authorized to carry out technical changes (e.g. firmware updates) beyond repair and replacement of defective parts in order to bring the equipment up to the current technical state. This does not result in any additional charges for the customer. A legal claim to this service does not exist.

2 Warranty period

The warranty period for ELSA products is six years. Excepted from this warranty period are ELSA color monitors and ELSA videoconferencing systems with a warranty period of 3 years. This period begins at the day of delivery from the ELSA dealer. Warranty services do not result in an extension of the warranty period nor do they initiate a new warranty period. The warranty period for installed replacement parts ends with the warranty period of the device as a whole.

3 Warranty procedure

- a) If defects appear during the warranty period, the warranty claims must be made immediately, at the latest within a period of 7 days.
- b) In the case of any externally visible damage arising from transport (e.g. damage to the housing), the transport company representative and ELSA should be informed immediately. On discovery of damage which is not externally visible, the transport company and ELSA are to be immediately informed in writing, at the latest within 7 days of delivery.
- c) Transport to and from the location where the warranty claim is accepted and/or the repaired device is exchanged, is at the purchaser's own risk and cost.
- d) Warranty claims are only valid if the original purchase receipt is returned with the device.

4 Suspension of the warranty

All warranty claims will be deemed invalid

- a) if the device is damaged or destroyed as a result of acts of nature or by environmental influences (moisture, electric shock, dust, etc.),
- b) if the device was stored or operated under conditions not in compliance with the technical specifications,

- c) if the damage occurred due to incorrect handling, especially to non-observance of the system description and the operating instructions,
- d) if the device was opened, repaired or modified by persons not authorized by ELSA,
- e) if the device shows any kind of mechanical damage,
- f) if in the case of an ELSA Monitor, damage to the cathode ray tube (CRT) has been caused especially by mechanical load (e.g. from shock to the pitch mask assembly or damage to the glass tube), by strong magnetic fields near the CRT (colored dots on the screen), or through the permanent display of an unchanging image (phosphor burnt),
- g) if, and in as far as, the luminance of the TFT panel backlighting gradually decreases with time, or
- h) if the warranty claim has not been reported in accordance with 3a) or 3b).

5 Operating mistakes

If it becomes apparent that the reported malfunction of the device has been caused by unsuitable software, hardware, installation or operation, ELSA reserves the right to charge the purchaser for the resulting testing costs.

6 Additional regulations

- a) The above conditions define the complete scope of ELSA's legal liability.
- b) The warranty gives no entitlement to additional claims, such as any refund in full or in part. Compensation claims, regardless of the legal basis, are excluded. This does not apply if e.g. injury to persons or damage to private property are specifically covered by the product liability law, or in cases of intentional act or culpable negligence.
- c) Claims for compensation of lost profits, indirect or consequential detriments, are excluded.
- d) ELSA is not liable for lost data or retrieval of lost data in cases of slight and ordinary negligence.
- e) In the case that the intentional or culpable negligence of ELSA employees has caused a loss of data, ELSA will be liable for those costs typical to the recovery of data where periodic security data backups have been made.
- f) The warranty is valid only for the first purchaser and is not transferable.
- g) The court of jurisdiction is located in Aachen, Germany in the case that the purchaser is a merchant. If the purchaser does not have a court of jurisdiction in the Federal Republic of Germany or if he moves his domicile out of Germany after conclusion of the contract, ELSA's court of jurisdiction applies. This is also applicable if the purchaser's domicile is not known at the time of institution of proceedings.
- h) The law of the Federal Republic of Germany is applicable. The UN commercial law does not apply to dealings between ELSA and the purchaser.

Declaration of conformity



KONFORMITÄTSERKLÄRUNG

DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:

This declaration is valid for the following product:

Geräteart:

Modem

Type of Device:

Typenbezeichnung:

MicroLink™ Cable

Product Name:

Hiermit wird bestätigt, daß das Erzeugnis den folgenden Schutzanforderungen entspricht:

This is to confirm that this product meets all essential protection requirements relating to the

Niederspannungs Richtlinie (73/23/EWG)

Low Voltage Directive (73/23/EEC)

EMV Richtlinie (89/336/EWG)

EMC Directive (89/336/EEC).

Zur Beurteilung der Konformität wurden folgende **Normen** herangezogen:

The assessment of this product has been based on the following **standards**

EN 50082-1: 1992 Teile/Parts: EN61000-4-2,3,4,6,11

EN 50081-1: 1992 Teile/Parts: EN 55022B+A1: 1995 +A2: 1997

EN 60950: 1992+ A1: 1993 +A2: 1993 +A3: 1995 +A4: 1997 +A11: 1997

Diese Erklärung wird verantwortlich für den Hersteller / Importeur

On behalf of the manufacturer / importer

ELSA AG

Sonnenweg 11

D-52070 Aachen

abgegeben durch

this declaration is submitted by

Aachen, 19. Juli 1999

Aachen, July 19th 1999

i.V. Peter Wieninger

Bereichsleiter Entwicklung

VP Engineering

Index

A

Access control	30
Access protocols	57
Access time	90
Access-list	93
Address Administration	17
Address administration	40
Address pool	42, 102
Address ranges	95
Apple Talk	52
ARP cache	93
ARP table	93
ARP-aging-minute(s)	94
Auto mode	102

B

Barring	30
Boot system	106
Bridge	
filtering data packets	40
Bridge	39
Bridge mode	90
Bridge table	90
Broadcast	90
Broadcast address	54
Broadcast data packets	90
Broadcast transfer	57
Brute force	29

C

Cable	50
Cable network	53
Cache	93
CE	7
Cells	50
Communities	25
Config-aging-minute(s)	104
Configuration	
Commands	19
SNMP	24
Configuration options	103

D

Data packet	50
Default route	95
Destination addresses	91
Destination network	95
Destination port	100
DHCP	40, 101
DHCP client	41
DHCP server	17, 41, 101
Display elements	1
Distance of a route	33
DNS	38, 93
DNS Forwarding	38
DNS server	40, 43
Domain Name Service	38
Dst-address	100
Dst-netmask	100
Dynamic Host Configuration Protocol	40
Dynamic IP routing table	97
Dynamic routing	32

E

Encryption	30
End address	42
End-address-pool	101
Exclusion routes	33

F

FCC	7
Filter	30
Filter-table	91
Filter-type	91
Firewall function	32
FirmSafe	22, 105
Firmware	104
Firmware Upload	
with LANconfig	23
Firmware upload	23
using TFTP	24
Firmware-upload	104
Flash ROM	22

G

Gateway 32, 40, 43

H

Heap reserve 90

Hierarchical IP addresses 55

Host 50

Hub 4

I

IANA 54

ICMP 96, 99

Inband 17

Requirements 17

using Telnet 18

Install software 22

Interface 50

Internet 31, 52

Internetwork 52

Inverse masquerading 98

IP 96

IP access list 17

IP address 17, 32, 92

IP addresses 53

IP broadcast 97

IP header 96

IP masquerading 30, 31, 36, 98

simple masquerading 37

supported protocols 38

IP multicast 97

IP network 52

IP routing

Filter 31

FTP 31

Telnet 31

IP routing table 32, 95

IP-netmask 92

IPX 52

ISDN network 53

L

LAN 52, 57

LAN-Coll 3

LANconfig 17, 18, 23

LAN-filter tab. 96

Language 104

LAN-Link 3

LAN-Rx 3

LAN-Tx 3

LED 1

Link Status LED 4

Loc. routing 96

Local Area Network 52

local network 52

Lock-minutes 104

Login 23, 30

Login barring 29

Log-in block 104

Login-errors 104

M

MAC 57

MAC address 89

MAC addresses 58

MAC protocol 58

Management Information Base 27

Manager 27

Masquerading 92, 98

Masquerading table 99

Media Access Control 57

Medium 50

MIB 25

Multicast 90

Multipoint cabling 57

Multiprotocol capability 58

N

Name 89

NAT 30, 31, 36

Netmask 53

Network 50

Network adapter 50

Network address 53

Network cable 50

Network connection 89

Network Information Center 36

Network protocol 52

NIC 36

- Node 4
- **O**
 - Objects 25
 - Online media 17
 - Operating 90, 92, 94
 - Operating modes 29
 - Other 106
- **P**
 - Packet 50
 - Password 93
 - Password protection 29
 - Password-required 104
 - PAT 30, 31, 36
 - Period of validity 41, 43
 - Physical medium 50
 - Point-to-multipoint connection 51
 - Point-to-point connection 50
 - Port number 38
 - PPP negotiation 92
 - Private address spaces 54
 - Prohibited address ranges 95
 - Protocol 52
 - Proxy ARP 95
- **R**
 - R1-mask 97
 - Registered IP address 54, 92
 - Remote station 90
 - RIP 97
 - RIP-type 97
 - Router 50
 - Router name 33
 - Routing 55
 - Routing table 55
- **S**
 - Security 29, 30, 32
 - Serial port 24
 - Service table 98
 - Setup
 - bridge-module 90
 - DHCP-module 101
 - IP-router-module 94
 - LAN-module 89
 - TCP-IP-module 91
 - WAN-module 89
 - Shared Medium 52, 57
 - Single user access 31
 - SNMP 24, 101
 - Agents 24
 - Manager 24
 - MIB 25
 - Source addresses 91
 - Source port 100
 - Start address 42
 - Start-address-pool 101
 - Static routing 32
 - Status 75
 - Config-statistics 88
 - IP-router-statistics 83
 - operating time 76
 - Queue-statistics 85, 87
 - TCP-IP-statistics 79
 - Subnet 55
 - System-administrator 101
 - System-location 101
- **T**
 - Table-RIP 97
 - TCP 99
 - TCP max. connections 94
 - TCP/IP 17, 32, 52
 - TCP/IP stack 52
 - TCP-aging-minute(s) 94
 - Technical data 63
 - Telnet server 93
 - TFTP 17
 - TFTP server 93
 - Time 76
 - Timeout 103
 - TOS 96
 - Trace
 - code and parameters 21
 - Examples 22
 - starting 21
 - Trace Outputs 21

Trap	27
Trap-IP	101
Traps-active	101
Type-of-service	96

U

UDP	99
Upload	22

Upload-system	106
---------------------	-----

V

Version-table	105
---------------------	-----

W

Wireless links	50
WWW	32

Description of the menu options

The menu tree for *ELSA MicroLink Cable* configuration is divided up into status information, setup parameters, firmware information and 'other'.

In order to help you familiarize yourself with the system, you will first be given an overview of the menu structure.

In the complete list of all menu options you will find a detailed description of all displays, menus and actions along with their associated parameters, default settings and input options.







You can access the menus when configuring via telnet or terminal programs and via SNMP (also see 'Configuration Modes').

When configuring with *ELSA LANconfig*, you are provided with an integrated help system that gives you brief descriptions of the individual parameters.

All channel-related statistics and menus in this documentation refer to two channels only, even if more than two channels are available to the specific devices. Interface-related information is also provided for a single interface only. The information is equally applicable to the additional channels and interfaces.













Symbols







	Menu	Indicates a further submenu.
	Info	Indicates a value that cannot be modified.
	Value	Indicates a value that can be modified.
	Table	Indicates a table whose entries can be modified.
	Info table	Indicates a table whose entries cannot be modified.
	Action	Performs an action.

Overview of the menus















Setup

-  Name
-  Cable-module
-  LAN-module
-  Bridge-module
-  TCP-IP-module
-  IP-router-module
-  SNMP-module
-  DHCP-server-module
-  Config-module
-  SYSLOG-module




Firmware

-  Version-table
-  Table-firmsafe
-  Mode-firmsafe
-  Timeout-firmsafe
-  Test-firmware
-  Firmware-upload

Status

-  Operating-time
-  Current-time
-  Cable-statistics
-  LAN-statistics
-  Bridge-statistics
-  TCP-IP-statistics
-  IP-router-statistics
-  Config-statistics
-  Queue-statistics
-  MCNS-statistics
-  Init-status
-  DHCP-client-status
-  Output-internal-status messages
-  Delete-values

Other

-  Boot-system
-  Factory-default-system
-  Upload-system

Status

The Status menu contains information on the current status and the internal sequences of operations in the LAN and in the cable network, which can relate to the data transmission route (e.g. registration with the headend) or to statistics (e.g. number of data blocks received and transmitted). The statistics displays are an important aid for verifying correct operation and optimizing parameter settings. In addition, they provide valuable information for error analysis when malfunctions occur.

Most status displays are continually updated and can be deleted with a **value** or set to 0 in the current menu.

The menu has the following layout:

Status		Running status displays
Operating-time		Period of time the device has operated since it was last switched on
Current-time		Current time in device
Cable-statistics		Display of statistics related to the cable network
LAN-statistics		Displays LAN statistics
Bridge-statistics		Bridge area statistics
TCP-IP-statistics		Statistics from the TCP/IP area
IP-router-statistics		Statistics from the IP router
Config-statistics		Remote configuration statistics
Queue-statistics		Statistics relating to the packets in the queues of the individual modules
MCNS-statistics		Statistics relating to MCNS packets and MCNS timeouts
Init-status		Status of initialization process
DHCP-client-status		Status of the DHCP client and the negotiated values
Info-connection		Information on the last connection for each interface
Layer-connection		Information on the B-channel protocol used for each interface
Channel-statistics		Information of the status of the individual channels
Time-statistics		Time module information
LCR-statistics		Least-cost router information
Output-internal-status messages		Query of the internal system status messages
Delete-values		Deletes all values except tables with substatistics.

Status/Operating-time

The operating time of the router since it was last started is displayed here in days, hours, minutes and seconds.

















Status/Current-time







This displays the current device time transferred by the headend.

Status/Cable-statistics

This option allows you to display the various statistics parameters for the cable network port. A large number of values related to the data volume transferred provide you with useful information on cable port load, errors that have occurred and the internal resources of the cable modems that are available in the current operating state.

















The **Status/cable-statistics** menu has the following layout:




/Cable-statistics		Running status displays
Cable-tx-discarded		Number of packets discarded due to an error/lack of resources
Cable-heap-packets		Number of buffers available
Cable-queue-packets		Number of buffers in use
Cable-queue-errors		Number of packets discarded due to a lack of buffers
Cable-tx-MAC-queue-packets		Number of buffers to be sent in the MAC chip
Cable-rx-MAC-queue-packets		Number of buffers for reception in the MAC chip
Cable-rx-fifo-full		Number of receive FIFO overruns
Cable-resp.-bandwidth-requests		Number of unanswered bandwidth request packets
Cable-rx-overflows-data-packets		Number of packets not received due to a lack of buffers
Cable-rx-overflows-Msg-packets		Number of control packets not received due to a lack of buffers
Cable-rx-CRC-mistake-packets		Number of control packets incorrectly received
Cable-rx-CRC-mistake-MCNS-header		Number of MCNS-header incorrectly received
Cable-tx-data packets		Number of data packets sent
Cable-rx-data packets		Number of data packets received
Cable-tx-msg-packets		Number of control packets sent
Cable-rx-msg-packets		Number of control packets received

/Cable-statistics		Running status displays
Cable-rx-MCNS-header-valid		Number of MCNS headers correctly received
Cable-FEC-lock-losses-not-recovered		Number of cable FEC lock losses not synchronized
Cable-FEC-lock-losses-recovered		Number of cable FEC lock losses resynchronized
Cable-TRC-lock-losses-not-recovered		Number of cable TRC lock losses not synchronized
Cable-TRC-lock-losses-recovered		Number of cable TRC lock losses resynchronized
Delete-values		Deletes Cable statistics

Status/LAN-statistics

Similarly to the previous menu option, this option allows you to display the statistics relating to the LAN connection. The **Status/LAN-statistics** menu has the following layout:

/LAN-statistics		Running status displays
LAN-rx-packets		Number of data packets received
LAN-tx-packets		Number of data packets sent
LAN-rx-errors		Number of data packets incorrectly received
LAN-tx-errors		Number of data packets incorrectly sent
LAN-stack-errors		Number of packets without a suitable receive module (bridge/router)
LAN-NIC-errors		Number of data packets discarded by the NIC
LAN-heap-packets		Number of buffers available
LAN-queue-packets		Number of buffers in use
LAN-queue-errors		Number of packets discarded due to a lack of buffers
LAN-collisions		Number of collisions during a send procedure
LAN-rx-bytes		Number of bytes received from the LAN
LAN-tx-bytes		Number of bytes sent to the LAN
LAN-rx-broadcasts		Number of broadcast packets received from the LAN
LAN-rx-multicasts		Number of multicast packets received from the LAN
LAN-rx-unicasts		Number of directly addressed packets received from the LAN
WAN-rx-broadcasts		Number of broadcasts received from the WAN

/LAN-statistics	Running status displays	
WAN-rx-multicasts		Number of multicasts received from the WAN
WAN-rx-unicasts		Number of unicasts received from the WAN
Delete-values		Deletes LAN statistics

Status/Bridge-statistics

This option allows you to display statistical information relating to the bridge. The bridge statistics contain the following parameters:
















/Bridge-statistics	Running status displays	
Brg-LAN-rx		Number of data packets received from the LAN
Brg-LAN-tx		Number of data packets sent to the LAN
Brg-LAN-filters		Number of filtered data packets by the LAN
Brg-LAN-broadcasts		Number of broadcasts received from the LAN
Brg-LAN-multicasts		Number of multicasts received from the LAN
BRG-Cable-rx		Number of data packets received from the cable network
BRG-Cable-tx		Number of data packets sent to the cable network
BRG-Cable-filters		Number of filtered data packets from the cable network
BRG-Cable-broadcasts		Number of broadcasts received from the cable network
BRG-Cable-multicasts		Number of multicasts received from the cable network
Brg-addresses		Number of addresses currently known
Brg-address-disc		Number of discarded CPEs
Brg-CPE-addresses		Number of CPEs permitted by the network operator
Table-bridge		Displays bridge filter table
Delete-values		Deletes bridge statistics








Table-bridge

The **bridge table** provides information on the MAC addresses known to the bridge, the time when the last packet was received from this device (specified in tics), and whether the relevant device is local or remote. This table is for internal bridge module use only and cannot be modified manually.

Node ID	Last-access	Forward-Flag
00a0570308e1	396442 tics	local
00a0570308e2	29442 tics	remote

Status/TCP-IP-statistics

The TCP/IP-related statistics are shown here, broken down according to the various TCP/IP sub-protocols. The TCP/IP statistics contain the following parameters:

/TCP-IP-statistics	Statistics from the TCP/IP area	
ARP-statistics		Statistics from the ARP area
IP-statistics		Statistics from the IP area
ICMP-statistics		Statistics for ICMP packets
TFTP-statistics		Statistics for TFTP operations
TCP-statistics		Statistics for TCP packets from TCP sessions to the router
DCHP-statistics		Statistics from the DHCP server
Delete-values		Deletes TCP/IP statistics

The substatistics then provide you with further parameters for the individual menus.

Status/TCP-IP-statistics/ARP-statistics

These statistics include the following values:

ARP-LAN-rx	Number of ARP requests and responses received from the LAN
ARP-LAN-tx	Number of ARP requests and responses sent to the LAN
ARP-LAN-errors	Number of ARP requests incorrectly received from the LAN
ARP-cable-rx	Number of ARP requests and responses received from the cable network
ARP-cable-tx	Number of ARP requests and responses sent to the cable network
ARP-cable-error	Number of ARP requests incorrectly received from the cable network
Table-ARP	Displays ARP table
Delete-values	Deletes ARP statistics

Table-ARP

There are 128 entries with ARP information in the **ARP table**. It has the following layout:

IP-address	Node ID	Last-access	Connect
IP address that has previously been found by ARP request	Associated MAC address	Time since the last access in tics	local or remote

Status/TCP-IP-statistics/IP-statistics

These statistics include the following values:

IP-LAN-rx	Number of IP packets received from the LAN
IP-LAN-tx	Number of IP packets sent to the LAN
IP-LAN-checksum-errors	Number of IP packets incorrectly received from the LAN
IP-LAN-service-errors	Number of IP packets received from the LAN for an incorrect service
IP-LAN-fragmentation-errors	Number of packets from the LAN that actually should have been fragmented prior to transmission due to their size, but which could not be fragmented.
IP-Cable-rx	Number of IP-packets received from the cable network
IP-Cable-tx	Number of IP-packets sent to the cable network
IP-Cable-checksum-errors	Number of IP packets incorrectly received from the cable network
IP-Cable-service-errors	Number of IP packets received from the cable network for an incorrect service
IP-Cable-fragmentation-errors	Number of packets from the cable network that actually should have been fragmented prior to transmission due to their size, but which could not be fragmented.
IP-Cable-rx-disconnect	Number of packets discarded by the cable network due to timeout
Delete-values	Deletes IP statistics

Status/TCP-IP-statistics/ICMP-statistics

These statistics include the following values:

ICMP-LAN-rx	Number of ICMP packets received from the LAN
ICMP-LAN-tx	Number of ICMP packets sent to the LAN
ICMP-LAN-checksum-errors	Number of ICMP packets incorrectly received from the LAN
ICMP-LAN-service-errors	Number of non-supported ICMP packets received from the LAN
ICMP-Cable-rx	Number of ICMP-packets received from the cable network
ICMP-Cable-tx	Number of ICMP-packets sent to the cable network
ICMP-Cable-checksum-errors	Number of ICMP packets incorrectly received from the cable network
ICMP-Cable-service-errors	Number of non-supported ICMP packets received from the cable network
Delete-values	Deletes ICMP statistics

Status/TCP-IP-statistics/TCP-statistics

These statistics include the following values:

TCP-LAN-rx	Number of TCP packets received from the LAN
TCP-LAN-tx	Number of TCP packets sent to the LAN
TCP-LAN-tx-repeats	Number of TCP packets repeatedly sent to the LAN
TCP-LAN-checksum-errors	Number of TCP packets incorrectly received from the LAN
TCP-LAN-service-errors	Number of TCP packets received from the LAN for an incorrect port
TCP-LAN-connections	Current number of TCP connections from the LAN
TCP-Cable-rx	Number of TCP-packets received from the cable network
TCP-Cable-tx	Number of TCP-packets sent to the cable network
TCP-Cable-tx-repeats	Number of TCP packets repeatedly sent to the cable network
TCP-Cable-checksum-errors	Number of TCP packets incorrectly received from the cable network
TCP-Cable-service-errors	Number of TCP packets received from the cable network for an incorrect port
TCP-Cable-connections	Current number of TCP connections from the WAN
Delete-values	Deletes TCP statistics

Status/TCP-IP-statistics/TFTP-statistics

These statistics include the following values:

TFTP-LAN-rx	Number of TFTP packets received from the LAN
TFTP-LAN-rx-read-request	Number of TFTP read requests received from the LAN
TFTP-LAN-rx-write-request	Number of TFTP write requests received from the LAN
TFTP-LAN-rx-data	Number of TFTP data packets received from the LAN
TFTP-LAN-rx-ack.	Number of TFTP acknowledges received from the LAN
TFTP-LAN-rx-option-ack.	Number of TFTP option acknowledges received from the LAN
TFTP-LAN-rx-errors	Number of TFTP error packets received from the LAN
TFTP-LAN-rx-bad-packets	Number of unknown TFTP packets received from the LAN
TFTP-LAN-tx	Number of TFTP packets sent to the LAN
TFTP-LAN-tx-data	Number of TFTP data packets sent to the LAN
TFTP-LAN-tx-ack.	Number of TFTP acknowledges sent to the LAN
TFTP-LAN-tx-option-ack.	Number of TFTP option acknowledges sent to the LAN
TFTP-LAN-tx-errors	Number of TFTP error packets sent to the LAN
TFTP-LAN-tx-repeats	Number of TFTP packets repeatedly sent to the LAN
TFTP-LAN-connections	Number of TFTP connections established to the LAN
TFTP-cable-rx	Number of TFTP-packets received from the cable network

TFTP-cable-rx-read-request	Number of TFTP read requests received from the cable network
TFTP-cable-rx-write-request	Number of TFTP write requests received from the cable network
TFTP-cable-rx-data	Number of TFTP data packets received from the cable network
TFTP-cable-rx-ack.	Number of TFTP acknowledges received from the cable network
TFTP-cable-rx-option-ack.	Number of TFTP option acknowledges received from the cable network
TFTP-cable-rx-errors	Number of TFTP error packets received from the cable network
TFTP-cable-rx-bad-packets	Number of unknown TFTP packets received from the cable network
TFTP-cable-tx	Number of TFTP packets sent to the cable network
TFTP-cable-tx-data	Number of TFTP data packets sent to the cable network
TFTP-cable-tx-ack.	Number of TFTP acknowledges sent to the cable network
TFTP-cable-tx-option-ack.	Number of TFTP option acknowledges sent to the cable network
TFTP-cable-tx-errors	Number of TFTP error packets sent to the cable network
TFTP-cable-tx-repeats	Number of TFTP packets repeatedly sent to the cable network
TFTP-cable-connections	Number of TFTP connections established to the cable network
Delete-values	Deletes TFTP statistics

Status/TCP-IP-statistics/DHCP-statistics

These statistics include the following values:

DHCP-LAN-rx	Number of DHCP packets received from the LAN
DHCP-LAN-tx	Number of DHCP packets sent to the LAN
DHCP-cable-rx	Number of DHCP packets received from the cable network
DHCP-discard	Number of DHCP packets discarded
DHCP-rx-discover	Number of discover messages received
DHCP-rx-request	Number of request messages received
DHCP-rx-decline	Number of decline messages received
DHCP-rx-inform	Number of inform messages received
DHCP-rx-release	Number of release messages received
DHCP-tx-offer	Number of offer messages sent
DHCP-tx-ack.	Number of DHCP packets acknowledged
DHCP-tx-nak.	Number of DHCP packets not acknowledged
DCHP-server-err.	Number of DHCP packets received that were not intended for this server
DHCP-assigned	Number of addresses currently assigned
DHCP-MAC-conflicts	Number of assignments rejected because IP addresses were in use
Table-DHCP	Table containing assignments of IP addresses to MAC addresses
Delete-values	Deletes DHCP statistics.




















Table-DHCP

There are entries with DHCP information in the **DHCP table**. It contains 16 entries (or multiples of 16). The table adapts dynamically to the given requirements and grows or shrinks accordingly. It has the following layout:

IP-address	Node ID	Timeout	Hostname	Type
IP address assigned via DHCP	Associated MAC address	Duration of assignment validity in minutes	Computer name	Assignment type

Status/IP-router-statistics

This menu groups together the statistics from the IP router module.

/IP-router-statistics	Statistics from the IP router area	
IPr-LAN-rx		Number of data packets to be routed from the LAN
IPr-LAN-tx		Number of data packets routed to the LAN
IPr-LAN-local-routings		Number of packets received from the LAN and routed to the LAN
IPr-LAN-network-errors		Number of LAN packets that were not routed
IPr-LAN-routing-errors		Number of LAN packets that must be sent to another router
IPr-LAN-ttl-errors		Number of LAN packets with an expired time-to-live value
IPr-LAN-filters		Number of LAN packets filtered by the filter table
IPr-LAN-discards		Number of LAN packets discarded
IPr-Cable-rx		Number of data packets to be routed from the cable network
IPr-Cable-tx		Number of data packets routed to the cable network
IPr-Cable-network-errors		Number of cable network packets that were not routed
IPr-Cable-ttl-errors		Number of cable network packets with an expired time-to-live value
IPr-Cable-filters		Number of cable network packets filtered by the filter table
IPr-Cable-discarded		Number of cable network packets discarded
IPr-Cable-type-errors		Number of packets from the cable network without an IP router ID
IPr-ARP-errors		Number of unsuccessful accesses to the ARP cache
Protocol-table		Table of routed packets arranged by protocol
RIP-statistics		Statistics from the IP/RIP area
Delete-values		Deletes IP router statistics

Protocol-table

The protocol table also supplies valuable information on the volume of packets transferred to the LAN or cable network. These values are broken down according to the various IP protocols, such as ICMP, TCP, UDP.

A protocol table might have the following appearance:

Protocol	LAN-tx	Cable-tx
tcp	14	30
udp	15	50
icmp	60	40

Status/IP-router-statistics/RIP-statistics

This option allows you to display the IP-RIP packets received by the device. These substatistics provide you with the following entries:

RIP-rx	Number of IP-RIP packets received
RIP-request	Number of IP-RIP request packets received
RIP-response	Number of IP-RIP response packets received
RIP-discards	Number of IP-RIP packets discarded
RIP-errors	Number of damaged IP-RIP packets
RIP-entry-errors	Number of erred entries in IP-RIP packets
RIP-tx	Number of IP-RIP packets sent
Table-IP-RIP	Routing table of routes learned through RIP broadcast
Delete-values	Deletes RIP statistics









The associated IP-RIP table contains all of the routes learned from the network. The router itself maintains this table; you cannot modify it manually.

An IP-RIP table might have the following appearance:

IP-address	IP-netmask	Time	Distance	Router
223.245.254.0	255.255.255.0	1	1	192.38.9.100
223.245.257.0	255.255.255.0	1	1	192.38.9.200













Status/Config-statistics














This menu allows you to display the statistics from the remote configuration area. It allows you to retrieve information on the number of past and present configuration sessions at any time. The information is broken down into the categories LAN, WAN and outband port.

/Config-statistics	Remote configuration statistics	
LAN-active-connections		Current number of active configuration connections from the LAN
LAN-total-connections		Total number of configuration connections from the LAN up until the present
Cable-active-connections		Current number of active configuration connections from the cable network
Cable-total-connections		Previous number of active configuration connections from the cable network
Login-errors		Total number of defective logins
Login-locks		Number of login locks
Login-rejects		Number of login attempts while the login lock was active
Delete-values		Deletes the config statistics















Status/Queue-statistics

These statistics allow you to observe the flow of the individual packets through the various modules of the devices.












/Queue-statistics	Statistics on the queue	
LAN-heap-packets		Number of buffers available
LAN-queue-packets		Number of buffers in use
Cable-heap-packets		Number of buffers available
Cable-queue-packets		Number of buffers in use
Bridge-internal-queue-packets		Number of bridge packets from the LAN
Bridge-external-queue-packets		Number of bridge packets from the WAN
ARP-query-queue-packets		Number of ARP packets in the query queue
ARP-queue-packets		Number of ARP packets in the normal queue
IP-queue-packets		Number of IP packets in the normal queue
IP-urgent-queue-packets		Number of IP packets in the secured queue
ICMP-queue-packets		Number of ICMP packets
TCP-queue-packets		Number of TCP packets




/Queue-statistics	Statistics on the queue	
TFTP-server-queue-packets		Number of packets in the receive queue of the TFTP server.
DHCP-server-queue-packets		Number of packets in the receive queue of the DHCP server.
DHCP-client-queue-packets		Number of packets in the receive queue of the DHCP clients
IPr-RIP-queue-packets		Number of packets in the receive queue of the IP-RIP module (for RIP queries, RIP propagations ...)
TFTP-queue-packets		Number of TFTP packets
Cable-tx-MAC-queue-packets		Number of packets to be sent in the MAC chip queue
Cable-rx-MAC-queue-packets		Number packet buffers for reception in the MAC chip queue
SNMP-queue-packets		Number of SNMP packets
TFTP-client-queue-packets		Number of packets in the receive queue of the TFTP clients
DNS-tx-queue-packets		Number of packets to be forwarded to DNS or NBNS servers
DNS-rx-queue-packets		Number of packets that come from DNS or NBNS servers and are to be forwarded to the host
IP-Masq.-tx-queue-packets		Number of packets to be sent masked (to the Internet)
IP-Masq.-rx-queue-packets		Number of packets received from the Internet and have to be demasked

Status/MCNS-statistics
















/MCNS-statistics		
MCNS-T1-timeouts		Number of timeouts while waiting for the upstream channel descriptor
MCNS-T2-timeouts		Number of broadcast ranging timeouts
MCNS-T3-timeouts		Number of ranging response timeouts
MCNS-T4-timeouts		Number of unicast ranging timeouts
MCNS-T6-timeouts		Number of registration response timeouts
MCNS-upstream-channel-descriptors		Number of received upstream channel descriptors
MCNS-ranging-requests		Number of ranging request packets were sent
MCNS-ranging-responses		Number of ranging response packets received
MCNS-ranging-aborts		Number of ranging aborts
MCNS-registration-requests		Number of registration request packets sent
MCNS-registration-responses		Number of registration response packets received
MCNS-SYNCS		Number of SYNC packets received
MCNS-Maps		Number of MAP packets received
Delete-values		Deletes MCNS statistics

Status/Init-status

/Cable-statistics		
Current-downstream-frequency		Display of the downstream frequency in Hz
Channel-found		Channel of the current downstream frequency found
Synchronization state		QAM, FEC and TRC synchronization
Upstream-descriptor-found		A suitable upstream configuration found in the downstream
Upstream power		Current transmission power in dBm
Ranging state		Status of the ranging process
DHCP state		Status of the DHCP negotiation
ToD state		Display of the Time-of-day negotiation
Configuration file state		Status of the configuration file download
Registration state		Status of the registration with the headend
Service ID		Service ID during and after registration






/Cable-statistics		
Class-ID		Class ID after registration
Upstream channel-ID		Number of the upstream channel
Downstream channel-ID		Number of the downstream channel





Status/DHCP-client-statistics

/DHCP-client-statistics		
State		Status of the DHCP client, on or off
Lease-time		Validity for the values assigned
Your-IP-address		IP address assigned by the headend
Your-IP netmask		IP netmask assigned by the headend
Gateway-IP-address		IP address assigned by the headend for BOOTP
Server-IP-address		Server IP address assigned by the headend
Security-server		Security server IP address assigned by the headend
Time-offset		Offset in seconds relative to GMT
Time-server		Currently used time server
Table-time-server		Table of time servers
Table-router		Table of routers
Table-name-server		Table of name servers
Table-domain-name-server		Table of domain name servers
Table-log-server		Table of log servers
Configuration file		Current configuration file

Setup

This menu allows you to query and modify all the system parameters that are necessary to the functioning of the devices.

/Setup		
System configuration		
Name		Entering the device name
Cable-module		Cable network settings
LAN-module		LAN settings
Bridge-module		Remote bridge settings
TCP-IP-module		TCP/IP module settings

/Setup		System configuration
IP-router-module		IP router module settings
SNMP-module		Settings for configuration via SNMP
DHCP-server-module		DHCP server settings
Config-module		Configuration module settings

Name

Here you can enter the device name (maximum 16 characters). The set of characters available includes uppercase and lowercase letters as well as some special characters. You can display the full range of available characters during a configuration session by entering the following command:

```
set \setup\name ?
```

In the default configuration, no name is entered.



Setup/Cable-module

This menu groups together all the settings necessary for starting up the interface to the cable network and for the connection to the headend.

These settings should only be changed by the cable network operator, as operation within the cable network will be impossible otherwise. The relevant menu items are therefore not covered in this documentation.

Setup/LAN-module





This menu item displays the connection values relevant for the local network. The menu has the following layout:

/LAN-module	LAN settings	
Connector		Network connection
Node-ID		MAC layer address of the device

This option allows you to display the router's own Ethernet address. The value displayed here was set at the factory and cannot be changed. The Ethernet address is displayed as a 12-digit hexadecimal value, with the first six digits '00a057' standing for an ELSA device.

Setup/Bridge-module

This menu allows you to select the settings necessary for bridge mode. The menu has the following layout:

/Bridge-module	Bridge settings	
Operating		Bridge active or inactive
Bridge-table		Displays bridge table.
LAN-config		Settings for the LAN side
Cable-config		Settings for the cable side

Operating

This option allows you to activate or deactivate the bridge. In the default configuration, the bridge is activated.



If the device is used just as an IP router connection, the bridge should be deactivated.

Bridge table

This option allows you to display the entries in the current bridge table. The table is automatically created and managed by means of a hash procedure. It comprises max. 512 entries.

Entries in the bridge table may appear as shown below when the bridge has acquired local and remote MAC addresses over time:

Node ID	Last-access	Forward-, Filter-Flag
00a05702000a	4 tics	local
0800096483D 4	105073354 tics	local
00001b157de0	105079059 tics	remote

The last access time to occur since the system was switched on is stored as a multiple of 9 ms (tics). The forward flag reflects the location of the MAC address. An entry in the form 00a057XXXXXX is the unique MAC address of the device.



The 'forward flag' column is output for remote configuration only. This column is not included in the display.

Broadcast

This option allows you to specify whether broadcast data packets are to be transmitted always (**pos** = default), never (**neg**), or only when a connection exists (**sem**).

Multicast

This option allows you to specify whether multicast data packets are to be transmitted always (**pos** = default), never (**neg**), or only when a connection exists (**sem**).



The **pos** setting for broadcast or multicast may lead to higher charges depending on the pricing model of the cable network operator during due to the higher data volume transferred.

Setup/Bridge-module/LAN-configuration/Dest.-addresses

This menu item enables all settings required to filter destination addresses.

/Dest.-address		Destination address filtering
Filter-type		Positive or negative filter
Filter-table		Processing of address filter table

Filter-type

The filter type to be used for the destination address list may be specified here. The settings **pos** are possible, so only data packets whose destination address is included in the destination address filter table will be transferred. The setting **neg** default value transfers all frames whose destination addresses are not included in the destination address filter table.

Filter-table

The destination addresses can be administered in this table. Entries simply comprise the **MAC-address** field.

Dest

0000c051d266

Setup/Bridge-module/LAN-configuration/Source-addresses

The settings for source addresses are made in the same way as the settings for the destination addresses.







Setup/Bridge-module/cable-configuration

This option allows you to select the settings for cable data packets. The settings in this menu are exactly the same as the settings in the **LAN-configuration** menu except that they serve to filter the data packets received from the cable network.

Setup/TCP-IP-module

This menu allows you to enter settings for the TCP/IP module. The menu has the following layout:

/TCP-IP-module		TCP/IP module settings
Operating		Activates or deactivates the TCP/IP module.
Cable IP address		IP address of the device in the cable network
Cable-IP-netmask		Cable network's matching IP network mask
LAN-IP-address		IP address for the device in the local network (LAN)

/TCP-IP-module		TCP/IP module settings
LAN-IP-mask		LAN's matching IP network mask
Access-list		Restricts access to internal functions via TCP/IP.
Table-ARP		ARP table for mapping an IP address onto a MAC address
ARP-aging-min.		Dwell time for entries in the ARP table
TCP-aging-min.		Time limit for configuration connections that are inactive
TCP-max.-conn.		Max. number of simultaneous configuration connections to the <i>ELSA MicroLink Cable</i>

Operating

The TCP/IP module of the router may be activated or deactivated here. In the default configuration, the TCP/IP module is activated.

Configuration via TCP/IP using Telnet and the IP router can only be used if the TCP/IP module is activated.

Cable IP address

The IP address for the device as transmitted by the headend during the registration is displayed here. The default address on delivery is '0.0.0.0'.

This IP address is used by the cable modem for the connection to the provider's (cable network operator) network.

IP netmask

The network mask belonging to the IP address must be entered here. The default setting is 255.255.255.0 (class C network). A network mask of 255.255.255.255 means that there is only one computer in this network (the router itself). This setting (an IP address registered in the Internet with a fully assigned network mask) can be used for masquerading via a raw IP access. With such an access an IP address is not assigned to the router by a PPP negotiation, but it must have a fixed IP address registered in the Internet.

Cable-IP-netmask

The netmask associated with the IP address as transmitted by the headend during the registration is displayed here.

LAN-IP-address

The LAN-side IP address for the device can be entered here. The second IP address enables the device to be used as a router for two logical IP networks and also this address has a specific meaning with the use of IP masquerading:

In this case, all computers that are in the network linked by the LAN-side IP address and IP netmask are "hidden" behind the address assigned by the provider (or the cable IP address).

LAN-IP-netmask

The network mask belonging to the IP address of the local network must be entered here. The default setting is 255.255.255.0 (class C network).



If no LAN-IP address has yet been specified, the device responds to a default IP address, the first three digits of which are identical to the first three digits of the sending device XXX.XXX.XXX.YYY. The device can then be reached by dialing the IP address XXX.XXX.XXX.254.

If such an IP address already exists in the network, shut down the device using the address for the duration of the configuration and assign a different, free LAN IP address to the cable modem.

Access-list

The access to "internal functions" of the router may be controlled by an access list in TCP/IP applications.



The configuration data of the device are protected by a password, however this is always transferred in plain text, making it possible in principle to detect it and for any computer to read the configuration or to delete it. In order to prevent this from happening, the access list can be used to determine which computers or which networks can access the configuration.

For reasons of consistency, the access control is based on all "internal functions" of the router. The term "internal functions" refers to the following:

- Telnet server: The configuration interface based on the Telnet protocol
- TFTP server: The configuration interface based on the TFTP protocol
- SNMP: the configuration interface based on the SNMP

Each of the maximum of 16 entries in the access list has the following structure:

IP-address	IP netmask
IP address of the authorized user (or user circle)	IP network mask of the user circle

Once an IP workstation with its IP address and the network mask 255.255.255.255 is entered into the list, the internal functions of the router can only be accessed from this computer. Any requests from devices with different IP addresses are ignored.

If a complete network has access enabled to a *ELSA MicroLink Cable*, this can be done as follows for a class C network:

IP-address	IP netmask
192.234.222.0	255.255.255.0

With this entry all IP addresses in the class C network 192.234.222.0 are authorized to use internal functions of the router.

ARP table

This option allows you to display the ARP table (ARP cache), which is managed automatically for the purpose of mapping IP addresses onto physical terminal addresses. Individual entries can be removed from this table but no new entries can be entered manually.

The entries in the ARP table might, for example, have the following appearance if different devices with different IP addresses (192.168.139.20, 192.168.130.30) communicated with the router:

IP-address	Node-ID	Last-access	Connect
192.168.130.20	0000c0717860	6780443 tics	local
192.168.130.30	0800091eebf4	6214514 tics	local

ARP-aging-min. This option allows you to enter a time (from 1 to 99 minutes) at the end of which the ARP table is automatically updated, i.e. all IP addresses that have not been accessed since the last automatic update are removed. The default setting is 15 minutes.

TCP-aging-min. If data transfer stops during a TCP connection to the router, e.g. if the user does not enter any more data during the remote configuration, it will automatically release the TCP connection on expiry of the time entered here. Possible settings are from 1 to 99 minutes; The default setting is 15 minutes.








TCP-max.-conn. The maximum number of allowable connections possible at the same time can be set here. DEFAULT setting is '0', meaning the same as "any number".

Setup/IP-router-module



This section describes the functions of the cable modem as an IP router. References in the following text to 'routers' thus refer to the cable modem in its IP router operating mode.

This menu allows you to enter settings for the IP router module. The menu has the following layout:

/IP-router-module	IP router module settings	
Operating		Activates or deactivates the IP router module.
IP-routing-table		Router table for IP network and remote station assignment
Loc.-routing		Activates/deactivates local routing
Routing-method		Routing method for IP packets
RIP-config		Settings for IP-RIP operation
Masquerading		Settings for IP masquerading
Firewall		Settings for firewall functions

Operating

This option allows you to activate or deactivate the IP router module. In the default configuration, the IP router module is activated.



Activating the IP router module also activates the TCP/IP module.

IP-routing-table The routing table can contain a maximum of 128 entries of destination network addresses or direct IP addresses with netmasks, and the names or IP addresses of other local routers. Alternatively, you can enter a setting by means of which packets to specific destination IP addresses are discarded and are not answered by proxy ARP. This is done by entering 0.0.0.0 for the name of the responsible router.

The IP routing table is generally sorted as shown below:

- The longest network mask is placed on top.
- For network masks of equal length, the one with the smallest IP address is placed on top.

Address ranges that are prohibited in the Internet are excluded from transmission by preset entries in the IP routing table (the router name 0.0.0.0 means that packets to these addresses are not transmitted). The IP routing table below is provided by way of example and also shows the default settings:

IP-address	IP netmask	Router-name	Distance
192.168.0.0	255.255.0.0	0.0.0.0	0
172.16.0.0	255.240.0.0	0.0.0.0	0
10.0.0.0	255.0.0.0	0.0.0.0	0
255.255.255.255	0.0.0.0	Cable TV network	0

However, if these addresses are required for Intranet use, for example, it is possible to delete the predefined entries at any time. If the routing table contains no entries with the router name 0.0.0.0, the router processes all IP addresses with valid routes.

The last line is an entry for the "default route". The IP address 255.255.255.255 means the same as 0.0.0.0 (for technical reasons, 0.0.0.0 cannot be entered in the first column). Because it contains the IP network mask 0.0.0.0, this line is always appropriate after the rest of the table has been searched. The router with the name 'Cable' stands for the cable network. The router thus sends everything that it cannot forward or transfer over other routes to the cable network operator's headend.

To route all data packets to a specific network, e.g. via an ISDN router in your LAN to another, enter the IP address of the other network and the netmask in the table and enter the local IP address of the router under 'Router'. The following assumes that your local network is using the IP addresses in the address range 10.1.0.0 (netmask 255.255.255.0). The ISDN router has the local IP address '10.1.0.99'; the other local network (that of your branch office) uses 10.2.0.0 (netmask 255.255.255.0). With the following entries, the cable modem will forward all data packets for the other network to the ISDN router and

sends all other data packets into the cable network (insofar as these are not in forbidden areas):

IP-address	IP netmask	Router-name	Distance
192.168.0.0	255.255.0.0	0.0.0.0	0
172.16.0.0	255.240.0.0	0.0.0.0	0
10.2.0.0	255.255.255.0	10.1.0.99	0
10.0.0.0	255.0.0.0	0.0.0.0	0
255.255.255.255	0.0.0.0	Cable	0



Loc. routing



Enable local routing for this function.

Local routing enables the router to forward data packets via the local network. The local routing is necessary if the router, as the default gateway for the workstations receives packets for destination networks to which it cannot establish a connection itself. If the router cannot return the address of the appropriate router to the workstation via ICMP, it will forward the data to the corresponding router itself (see also 'Local Routing'). Since this setting increases network utilization in the LAN, the default setting is 'Off'.

Setup/IP-router-module/Routing-method

The router offers two methods for IP routing, which can be separately set for IP and ICMP packets. Both methods are based on the evaluation of the field 'Type-of-service' in the IP header.

The menu has the following layout:

/Routing-method	Routing method settings	
Routing-method		Routing method for IP packets
ICMP-routing-method		Routing method for ICMP packets

Routing-method This option allows you to define the routing method used for IP packets:

- If you select 'Normal', all IP packets are handled in the same way as per the routing specifications of the Internet protocol.
- If you select 'Type-of-service', IP packets are placed in the urgent queue or reliable queue, depending on the contents of the 'Type-of-service' field. All other packets are placed in the normal send queue. In this way, transmission is guaranteed, provided that it is possible.




ICMP-routing-method

This option allows you to define the routing method used for ICMP packets:

- If you select 'Normal', the ICMP packets are handled like any other IP packets as per the routing specifications of the Internet protocol.
- If you select 'Reliable', all ICMP packets received are placed in the reliable queue.

Setup/IP-router-module/RIP-configuration

This option allows you to enter settings for the management of IP-RIP packets. The menu has the following layout:

/RIP-configuration		Settings for IP-RIP operation
RIP-type		RIP compatibility switch
R1-mask		Management of network masks
Table-IP-RIP		Dynamic IP routing table

RIP-type

This option allows you to select the method to be used for handling the IP-RIP packets. The different settings have the following meaning:

- **Off:** IP-RIP is not supported (default).
- **RIP-1:** RIP-1 and RIP-2 packets are received but only RIP-1 packets are sent.
- **R1-comp:** RIP-1 and RIP-2 packets are received. RIP-2 packets are sent as an IP broadcast.
- **RIP-2:** Same as **R1-comp** except that all RIP packets are sent to the IP multicast address 224.0.0.9.

R1-mask

If **RIP-1** is set, this option allows you to influence the management of network masks. Therefore, these settings are required only for subnetting under **RIP-1**. The different settings have the following meaning:

- **Class** (default): The network mask used in the RIP packet is derived directly from the IP address class, i.e. the following network masks are used for the network classes:
 - Class A: 255.0.0.0
 - Class B: 255.255.0.0
 - Class C: 255.255.255.0
- **Address:** The network mask is derived from the first bit that is set in the IP address entered. This and all high-order bits within the network mask are set. Thus, for example, the address 127.128.128.64 yields the IP network mask 255.255.255.192.
- **Cl+Addr:** The network mask is formed from the IP address class and a part attached using the address procedure. Thus, the above-mentioned address and the network mask 255.255.0.0 yield the IP network mask 255.128.0.0.

Table-IP-RIP

This option allows you to display the entries in the current dynamic IP routing table.

An IP-RIP routing table might, for example, have the following appearance:







IP-address	IP netmask	Time	Distance	Router
223.245.254.0	255.255.255.0	1	1	192.38.9.100
223.245.257.0	255.255.255.0	1	1	192.38.9.200

Cable-RIP
LAN-RIP

Select whether RIP packets should be sent into the LAN or cable network here.

Setup/IP-router-module/Masquerading

This menu allows you to enter settings for the masquerading function. The menu has the following layout:

/Masquerading	Settings for IP masquerading	
Operating		Masquerading function on or off
TCP-aging-second(s)		Time in seconds after which a TCP masquerading becomes invalid
UDP-aging-second(s)		Time in seconds after which a UDP masquerading becomes invalid
ICMP-aging-second(s)		Time in seconds after which an ICMP masquerading becomes invalid
Service-table		Static masquerading table
Table-masquerading		Dynamic masquerading table

Service-table

The use of inverse masquerading makes 'services' (e.g. a file server) selectively visible in the Internet by entering specified ports in the service table in the IP network, while all other services and computers remain invisible from the local network (see also 'IP Masquerading (NAT, PAT)' on page 31). The service table (also called the static masquerading table) can contain up to 16 entries and has the following layout:

D-port	Intranet-addr.
20	10.1.1.10
21	10.1.1.10

The different columns have the following meaning:

- D-port: Destination port for the particular entry
- Intranet-addr.: Destination IP address for the computer in the local network

Through this assignment, it is possible, for example, to address the relevant service directly via telnet. Enter the IP address of the router and attach the port number, separated by a colon, to the address.

You can use the command

```
telnet 192.38.50.100:27
```

to connect directly to a news server that can be reached via a router with the IP address 192.38.50.100.

Table-masquerading

With IP masquerading, the IP addresses of computers in the local network are rendered invisible to external devices by means of a conversion of addresses and ports in the router. The dynamic masquerading table displays the IP addresses from the local network that the router is currently masking. The dynamic masquerading table can contain up to 2048 entries and has the following layout:

Intranet-addr.	S-port	Protocol	Timeout
10.1.1.10	1234	TCP	10

The different columns have the following meaning:

- Intranet-addr.: IP address of the computer in the local network
- S-port: Source port for this entry
- Protocol: Protocol used (TCP/UDP/ICMP)
- Timeout: Time in seconds until the entry is removed from the table

Setup/IP-router-module/firewall

The filters for the IP packets are set in this menu.

The IP filters are defined in a table with the following layout:

Idx.	Active	Prot	Src-address	Src-netmask	S-st.	S-end	Dst-address
WIN	YES	TCP	255.255.255.255	0.0.0.0	137	139	0.0.0.0

Dst-netmask	D-st.	D-end	Action	Ifc	Direct.	MBUcst	Matches
0.0.0.0	53	53					

The table fields have the following meaning:

- Idx.
Unique index. This entry is required to distinguish the filters. The index may be four characters long and selected as desired.
- Active
Activates or deactivates the filter.
- Prot
Protocol that is to be filtered. Possible entries are **TCP**, **UDP**, **ICMP** and **all**.

The setting **all** filters out every packet from the specified source network or to the destination network

■ Src-address, Src-netmask

A subnetwork of the local network for which the filter is valid can be entered here. A source address of 0.0.0.0 means that the filter is applied to all computers. A network mask of 0.0.0.0 means that the filter is applied to all networks (which also means all computers).

■ S-st., S-end

Source port range that is to be filtered. A range of 0 to 0 means that no source port is affected by this filter.

■ Dst-address, Dst-netmask

A subnetwork of the local network for which the filter is valid can be entered here. A destination address of 0.0.0.0 means that the filter is applied to all computers. A network mask of 0.0.0.0 means that the filter is applied to all networks (which also means all computers).

■ D-st., D-end

Destination port range that is to be filtered. A range of 0 to 0 means that no destination port is affected by this filter.

■ Action

The filter can discard (not forward) or accept (forward) packets.

■ Interface

Select whether the filter should apply to the LAN interface, the interface to the cable TV network, or both.

■ Direction

Select whether the filter should apply to incoming, outgoing, or all packets.

■ Broadcast

Select whether all broadcast packets (including unicast) or only multi/broadcast packets should be filtered.

■ Number (matches)

Number of packets that fit the filter.

The table entries are sorted in a similar fashion to the IP router table:

■ The longest network mask is placed on top.





■ For two network masks of equal length, the one with the smallest IP address is placed on top.

Network masks and IP addresses of 0.0.0.0 can be used as “wildcards”. Specified computers and networks may be simultaneously subjected to targeted filtering while others pass the router unfiltered.

The tables are processed from top to bottom. As soon as a matching filter is found, the packet is handled accordingly.

Setup/SNMP-module

This menu allows you to enter settings for configuration of the device via SNMP. The menu has the following layout:

/SNMP-module		SNMP module settings
Send-Traps		Switch for issuing SNMP traps
IP-Trap-Table		Table with 20 destination addresses for trap messages
Administrator		Device administrator
Location		Device location

Send-Traps This entry controls trap output (No/Yes).









IP-Trap-Table Specifies the IP addresses to which the trap messages will be sent.

Administrator Administrator's name

Location Device location

Setup/DHCP-server-module

This menu allows you to enter settings for the DHCP server. The menu has the following layout:

/DHCP-server-module		DHCP server settings
Operating		Switch for activating the DHCP module
Start-address-pool		Start address for the address pool
End-address-pool		End address for the address pool
Netmask		Network mask for the address pool
Broadcast-address		Broadcast address for the LAN
Max.-lease-time-minute(s)		Maximum period of validity for the address assignment via DHCP
Default-lease-time-minute(s)		Default period of validity for the address assignment via DHCP
Table-DHCP		Table of current assignments via DHCP

Operating On: The device operates as a DHCP server.

Off: The device does not operate as a DHCP server.

Auto: The device regularly checks whether there is another DHCP server in the LAN. If not, it operates as a DHCP server and issues IP addresses to local clients.



If there is no cable or LAN-IP address entered in the TCP/IP module (e.g. factory setting), the cable modem will issue IP addresses from the address range 10.0.0.2 - 10.0.0.253 to all DHCP clients in auto mode.

*Start-address-pool
End-address-pool*

The IP address assigned is taken from the address pool selected ('Start-address-pool' to 'End-address-pool'). Any valid addresses in the local network can be entered here.

If 0.0.0.0 is entered instead, the device will determine the appropriate addresses (start or end) from the settings under 'Setup/TCP module'. The procedure is as follows:

- If only the cable or LAN-IP address is entered, the start or end of the pool is determined by means of the associated network mask.
- If both addresses have been specified, the LAN-IP address has priority for determining the pool.
- The start address of the pool is either the address given in the DHCP module or the first valid address in the local network.
- The end address of the pool is either the address given in the DHCP module or the last valid address in the local network.

A valid address is then taken from the IP address pool. If the computer was already assigned an IP address at some point in the past, it requests this same address and the DHCP server attempts to reassign this address if it has not already been assigned to another computer.

The DHCP server also checks whether the address that is to be assigned to the computer is unique in the local network. It does this by issuing an ARP request to the address. If the ARP request is answered, the DHCP server begins the procedure again with a new address. As soon as the uniqueness of an address has been established, the requesting computer is assigned the address found.

Netmask

The network mask is assigned in the same way as the IP address:

The system either assigns the network mask entered in the DHCP module or uses the network mask that belongs to the local network (determined during address assignment).

Broadcast

The broadcast address is assigned in the same way as the IP address:

The system either assigns the broadcast address entered in the DHCP module or uses the broadcast address that belongs to the local network (determined during address assignment).

Max.-lease-time-minute(s)

Here you can enter the maximum period of validity that the DHCP server assigns a host.

The DEFAULT value of 6000 minutes equals approximately 4 days.

Default-lease-time-minute(s) Here you can enter the period of validity that is assigned if the host makes no request. The DEFAULT value of 500 minutes equals approximately 8 hours.

Table-DHCP In the DHCP module, the 'Table-DHCP' option allows you to verify (or look up) the assignment of IP addresses to the relevant computers. This table has the following layout:

IP-address	Node-ID	Timeout	Hostname	Type
10.1.1.10	00a0570308e1	500	ELSA	new





- IP-address: IP address assigned
- Node-ID: The computer's Ethernet address
- Timeout: Time remaining until the assignment becomes invalid
- Hostname: The computer's name in plain text if it was transmitted in the request
- Type: This field contains additional information on the assignment.




The 'Type' field specifies how the address was assigned. This field can assume the following values:

- **new**: The computer has made its initial request. The DHCP server verifies the uniqueness of the address that is to be assigned to the computer.
- **unkn.**: While verifying uniqueness, it was determined that the address has already been assigned to another computer. Unfortunately, the DHCP server has no means of obtaining additional information on this computer.
- **stat.**: A computer has informed the DHCP server that it has a fixed IP address. This address can no longer be used.
- **dyn.**: The DHCP server assigned an address to the computer.

Setup/Config-module

This menu allows you to enter settings for router configuration options. The menu has the following layout:

/Config-module		Configuration module settings
Password-required		Password required on/off if there is no password
Switch-Off-mode		Configuration of the On/Standby switch
Standby		Standby status
Config-aging-minute(s)		Time limit for remote configuration connections

/Config-module	Configuration module settings	
Login-errors		Number for failed log-in attempts before the log-in block is activated
Lock-minutes		Duration of block and period until old log-in errors are forgotten.
Language		Configuration language

Password-required

This specifies whether a new password should be requested every time a configuration is begun (**On**), or the password request should be suppressed (**Off**). The default setting for this option is **Off**.

Config-aging-minute(s)

If data transmission halts during a remote configuration session, e.g. because the user is no longer entering data, the device automatically releases the connection at the end of the time period specified here. Possible settings are from 1 to 99 minutes. The default setting is 15 minutes.

Login-errors

This entry specifies the number of failed attempts allowed before the log-in block is activated. An empty password (simply pressing <ENTER> at the password prompt) is not considered an attempt and therefore does not activate the block.



The default value is 5. A lower value may cause the log-in block to be activated with only one access on an older ELSA LANconfig! In this case obtain an updated ELSA LANconfig version from our online sources.

Lock-minutes




This entry has two meanings. It indicates how long the access is blocked if the log-in block has been activated. It also sets the period after which the device forgets all prior login errors.




Language

This option allows you to select whether you will use the German or English version of the software for performing the configuration.

Firmware

This menu allows you to display various firmware parameters and to initiate a firmware upload:

/Firmware	Display and keyboard settings	
Version-table		Displays hardware releases and serial numbers for the cable modem
Table-firmsafe		Information on the two firmware versions stored in the device and on the bootloader
Mode-firmsafe		Firmware activation mode

/Firmware		Display and keyboard settings
Timeout-firmsafe		Time in minutes required to test new firmware
Test-firmware		Tests the inactive firmware
Firmware-upload		Initiates a firmware upload

Version table The version table displays the firmware version and serial number of the device.

lfc	Module	Version	Serial-number
lfc	MicroLink Cable	1.00 22.03.99	0317.000.005

Table firmsafe This table provides the following details for the two firmware versions stored in the device: the position in memory (1 or 2), status information (active or inactive), the version number, the date, the size and the index (sequential number).

Position	Status	Version	Date	Size	Index
1	Inactive	1.60	23061999	690	6
2	Active	1.60	30061999	692	7
3	<loader>	1.60	07061999	64	0

Enter the following command to activate an inactive firmware version:

```
set <position number> active
```




Mode-firmsafe Only one of the two firmware versions stored in the device can be active at any one time. When new firmware is loaded, the inactive firmware is overwritten. You can decide which firmware will be activated after the upload:

- 'immediate': The first option is to load the new firmware and activate it immediately. The following situations can result:
 - The new firmware is successfully loaded and then operates as desired. Everything is then in order.
 - However, if the new firmware does not operate correctly, it may not be possible to communicate with the device after the restart. If an error occurs during the upload, the device automatically reactivates the previous firmware version and reboots the device.
- 'login': To prevent problems caused by defective firmware, the second option will load the firmware and start it immediately.
 - In contrast to the first option, the firmsafe will wait until it has successfully logged on (via telnet). The new firmware will only be permanently activated when the login occurs successfully within the time set under 'Timeout firmsafe'.

- If the device no longer responds and it is therefore impossible to log in, the firmware automatically loads the previous firmware version and reboots the device with it.
- 'manual': The third option allows you to set a period (Timeout firmsafe) beforehand for testing the new firmware. The device will start with the new firmware and wait for the preset period until the loaded firmware is manually activated and therefore becomes permanently effective.

Other

The **Other** menu allows you to manage the following functions:

/Other	Various functions	
Boot-system		Boots the device
Factory-default-system		Resets to factory settings
Upload-system		Loads new firmware

Boot-system

This option allows you to reboot the device.



Before executing the command all open connections will be released or closed. The device must log back on with the network operator after rebooting.

Factory-default-system

This option resets all the settings that have been entered. The device is reset to the factory settings.

For security reasons, the system prompts you to enter the configuration protection password in order to ensure that you have not mistakenly selected this command instead of the `Boot-system` command. If no password has been assigned, you must press Enter a second time.

Upload-system

This option starts a firmware upload (refer to chapter 'How to load new software').

The flash ROM technology permits flexible and service-friendly handling of the system software by allowing different firmware versions to be read in. It also allows devices to be retrofitted with all future options.